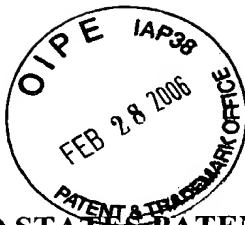


Docket No. 205483US2X



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Ken UMENO

GAU: 2637

SERIAL NO: 09/820,826

EXAMINER: TSE, Y.

FILED: March 30, 2001

FOR: PSEUDO-RANDOM NUMBER SEQUENCE OUTPUT UNIT, TRANSMITTER,
RECEIVER, COMMUNICATION SYSTEM AND FILTER UNIT

SUBMISSION NOTICE REGARDING PRIORITY DOCUMENT(S)

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

Certified copies of the Convention Application(s) corresponding to the above-captioned matter:

☒ are submitted herewith

☐ were filed in prior application filed

☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule
17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Registration No. 25,599
Kurt M. Berger, Ph.D.
Registration No. 51,461

Customer Number
22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 11/04)
GJM:KMB:fb1
I:\ATTY\KMB\205's\205483US\205483.PRIORITY REQ.DOC

日本国特許庁
JAPAN PATENT OFFICE

6329 05

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日 2000年 4月 7日
Date of Application:

出願番号 特願2000-107047
Application Number:

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願

country code and number
of our priority application,
which is used for filing abroad
under the Paris Convention, is

J P 2000-107047

願 人
Applicant(s):

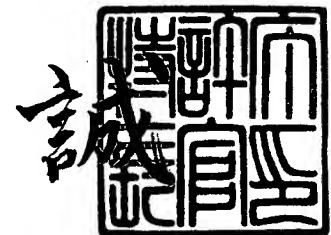
独立行政法人情報通信研究機構
梅野 健

CERTIFIED COPY OF
PRIORITY DOCUMENT

2005年10月17日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋



BEST AVAILABLE COPY

出証番号 出証特2005-3086273

【書類名】 特許願

【整理番号】 CRL-00-A

【提出日】 平成12年 4月 7日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/00

【発明者】

【住所又は居所】 東京都小金井市貫井北町 4 丁目 2 番 1 号 郵政省通信総合研究所内

【氏名】 梅野 健

【特許出願人】

【識別番号】 391027413

【氏名又は名称】 郵政省通信総合研究所長 飯田 尚志

【特許出願人】

【識別番号】 597044841

【氏名又は名称】 梅野 健

【代理人】

【識別番号】 100095407

【弁理士】

【氏名又は名称】 木村 満

【選任した代理人】

【識別番号】 100110135

【弁理士】

【氏名又は名称】 石井 裕一郎

【手数料の表示】

【予納台帳番号】 038380

【納付金額】 10,500円

【その他】 国以外のすべての者の持分の割合 0 5 0 / 1 0 0

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置、擬似乱数列の出力方法、送信方法、受信方法、フィルタ方法、ならびに、情報記録媒体

【特許請求の範囲】

【請求項 1】

s ($1 \leq s$) 個の所定の正整数 q_1, q_2, \dots, q_s と、所定の実インパルス定数 r ($-1 < r < 1$) と、に対して、長さ N ($1 \leq N$) の擬似乱数列を出力する擬似乱数列の出力装置であって、

s ($1 \leq s$) 個の実数の系列初期値 Y_1, Y_2, \dots, Y_s ($-1 < Y_1 < 1, -1 < Y_2 < 1, \dots, -1 < Y_s < 1$) と、

s 個の整数パラメータ p_1, p_2, \dots, p_s ($2 \leq p_1, 2 \leq p_2, \dots, 2 \leq p_s$) であって、そのそれぞれについて、前記所定の正整数 q_1, q_2, \dots, q_s に対して、 $q_1 \bmod p_1 \neq 0, q_2 \bmod p_2 \neq 0, \dots, q_s \bmod p_s \neq 0$ が成立する s 個の整数パラメータと、の入力を受け付ける入力受付部と、

前記所定の実インパルス定数 r と、前記系列初期値 Y_1, Y_2, \dots, Y_s と、前記整数パラメータ p_1, p_2, \dots, p_s と、前記所定の正整数 q_1, q_2, \dots, q_s と、整数 j ($1 \leq j \leq s$), m ($1 \leq m \leq 2N-2$), n ($1 \leq n \leq 2N-1$) と、についての漸化式

【数 1】

$$T_p(\cos \theta) = T(p, \cos \theta) = \cos(p\theta)$$

$$y_j[1] = Y_j$$

$$y_j[m+1] = T(p_j, y_j[m])$$

$$z[n] = \prod_{j=1}^s T(q_j, y_j[n])$$

から、長さ N の擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ であって、

【数 2】

$$\begin{aligned}
 z'[1] &= \sum_{j=1}^N (-r)^j z[j], \\
 z'[2] &= \sum_{j=1}^N (-r)^j z[j+1], \\
 &\vdots \\
 z'[N] &= \sum_{j=1}^N (-r)^j z[j+N-1]
 \end{aligned}$$

を満たす擬似乱数列 $z'[1]$, $z'[2]$, ..., $z'[N]$ を計算する計算部と、
前記擬似乱数列 $z'[1]$, $z'[2]$, ..., $z'[N]$ を出力する出力部と、
を備えることを特徴とする出力装置。

【請求項 2】

前記系列初期値 Y_1 , Y_2 , ..., Y_s は、整数 k ($1 \leq k \leq s$)と、整数 m ($1 \leq m \leq N$)と、
に対して

【数 3】

$$\begin{aligned}
 y_k[2] &= T(p_k, Y_k) \\
 y_k[m+1] &= T(p_k, y_k[m]) \\
 Y_k &= y_k[N+1] = T(p_k, y_k[N])
 \end{aligned}$$

を満足することを特徴とする請求項 1 に記載の出力装置。

【請求項 3】

前記所定の実インパルス定数 r は、

【数 4】

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

を満足する

ことを特徴とする請求項 1 または 2 に記載の出力装置。

【請求項 4】

前記所定の正整数 q_1, q_2, \dots, q_s は、いずれも 1 である

ことを特徴とする請求項 1 から 3 のいずれか 1 項に記載の出力装置。

【請求項 5】

伝送信号の入力を受け付ける入力受付部と、

請求項 1 から 4 のいずれか 1 項に記載の長さ N の擬似乱数列を出力する出力装置と、

前記入力を受け付けられた伝送信号を、前記出力された長さ N の擬似乱数列を拡散符号として、スペクトラム拡散する拡散部と、

前記スペクトラム拡散された結果の信号を送信する信号送信部と、

を備えることを特徴とする送信装置。

【請求項 6】

系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を選択する選択部と、

前記選択された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を送信するパラメータ送信部と、

をさらに備え、

前記出力装置は、前記選択された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、の入力を受け付けて、長さ N の擬似乱数列を出力する

ことを特徴とする請求項 5 に記載の送信装置。

【請求項 7】

系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を受信するパラメータ受信部と、

をさらに備え、

前記出力装置は、前記受信された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、の入力を受け付けて、長さ N の擬似乱数列を出力する

ことを特徴とする請求項 5 に記載の送信装置。

【請求項 8】

信号を受信する信号受信部と、

請求項 1 から 4 のいずれか 1 項に記載の長さ N の擬似乱数列を出力する出力装

置と、

前記受信された信号を、前記出力された長さNの擬似乱数列を拡散符号として、
スペクトラム逆拡散する逆拡散部と、
前記スペクトラム逆拡散された結果の信号を伝送信号として出力する出力部と、
を備えることを特徴とする受信装置。

【請求項 9】

系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を選択する
選択部と、

前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S
と、を送信するパラメータ送信部と、
をさらに備え、

前記出力装置は、前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、のを受け付けて、長さNの擬似乱数列を出力する
ことを特徴とする請求項 8 に記載の受信装置。

【請求項 10】

系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を受信する
パラメータ受信部と、
をさらに備え、

前記出力装置は、前記受信された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、のを受け付けて、長さNの擬似乱数列を出力する
ことを特徴とする請求項 8 に記載の受信装置。

【請求項 11】

請求項 6 に記載の送信装置と、
請求項 10 に記載の受信装置と、
を備え、
前記受信装置は、前記送信装置から送信された系列初期値 Y_1, Y_2, \dots, Y_S と、
整数パラメータ p_1, p_2, \dots, p_S と、を受信し、
前記受信装置は、前記送信装置から送信された信号を受信する

ことを特徴とする通信システム。

【請求項 12】

請求項 7 に記載の送信装置と、

請求項 9 に記載の受信装置と、

を備え、

前記送信装置は、前記受信装置から送信された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を受信し、

前記受信装置は、前記送信装置から送信された信号を受信する

ことを特徴とする通信システム。

【請求項 13】

所定の実インパルス定数 r ($-1 < r < 1$) に対するフィルタ装置であって、

チップ長 D の入力信号の入力を受け付ける入力端子と、

前記入力を受け付けられた入力信号を、それぞれ $0, D, 2D, 3D, \dots, (N-1)D$ だけ遅延させた複数の信号を出力する遅延部と、

前記遅延されて出力された複数の信号のそれぞれを、当該遅延時間が T である場合、 $(-r)^{(N-T)/D}$ 倍して出力する増幅部と、

前記増幅されて出力された複数の信号の総和を出力する加算部と、

前記加算されて出力された信号を出力する出力端子と、

を備えることを特徴とするフィルタ装置。

【請求項 14】

前記フィルタ装置の遅延部、増幅部、および、加算部は、ASIC (Application Specific Integrated Circuit)、DSP (Digital Signal Processor)、もしくは、FPGA (Field Programmable Gate Array) によって構成されることを特徴とする請求項 13 に記載のフィルタ装置。

【請求項 15】

s ($1 \leq s$) 個の所定の正整数 q_1, q_2, \dots, q_s と、所定の実インパルス定数 r ($-1 < r < 1$) と、に対して、長さ N ($1 \leq N$) の擬似乱数列を出力する擬似乱数列の出力方法であって、

s ($1 \leq s$) 個の実数の系列初期値 Y_1, Y_2, \dots, Y_s ($-1 < Y_1 < 1, -1 < Y_2 < 1, \dots$,

$-1 < Y_S < 1$) と、

s 個の整数パラメータ p_1, p_2, \dots, p_s ($2 \leq p_1, 2 \leq p_2, \dots, 2 \leq p_s$) であって、そのそれぞれについて、前記所定の正整数 q_1, q_2, \dots, q_s に対して、 $q_1 \bmod p_1 \neq 0, q_2 \bmod p_2 \neq 0, \dots, q_s \bmod p_s \neq 0$ が成立する s 個の整数パラメータと、
 の入力を受け付ける入力受付工程と、

前記所定の実インパルス定数 r と、前記系列初期値 Y_1, Y_2, \dots, Y_S と、前記整数パラメータ p_1, p_2, \dots, p_s と、前記所定の正整数 q_1, q_2, \dots, q_s と、整数 j ($1 \leq j \leq s$), m ($1 \leq m \leq 2N-2$), n ($1 \leq n \leq 2N-1$) と、についての漸化式

【数 5】

$$T_p(\cos \theta) = T(p, \cos \theta) = \cos(p\theta)$$

$$y_j[1] = Y_j$$

$$y_j[m+1] = T(p_j, y_j[m])$$

$$z[n] = \prod_{j=1}^s T(q_j, y_j[n])$$

から、長さ N の擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ であって、

【数 6】

$$z'[1] = \sum_{j=1}^N (-r)^j z[j],$$

$$z'[2] = \sum_{j=1}^N (-r)^j z[j+1],$$

\vdots

$$z'[N] = \sum_{j=1}^N (-r)^j z[j+N-1]$$

を満たす擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ を計算する計算工程と、

前記擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ を出力する出力工程と、

を備えることを特徴とする出力方法。

【請求項 16】

前記系列初期値 Y_1, Y_2, \dots, Y_s は、整数 k ($1 \leq k \leq s$)と、整数 m ($1 \leq m \leq N$)と、
に対して

【数 7】

$$\begin{aligned} y_k[2] &= T(p_k, Y_k) \\ y_k[m+1] &= T(p_k, y_k[m]) \\ Y_k &= y_k[N+1] = T(p_k, y_k[N]) \end{aligned}$$

を満足することを特徴とする請求項 15 に記載の出力方法。

【請求項 17】

前記所定の実インパルス定数 r は、

【数 8】

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

を満足する

ことを特徴とする請求項 15 または 16 に記載の出力方法。

【請求項 18】

前記所定の正整数 q_1, q_2, \dots, q_s は、いずれも 1 である

ことを特徴とする請求項 15 から 17 のいずれか 1 項に記載の出力方法。

【請求項 19】

伝送信号の入力を受け付ける入力受付工程と、

請求項 15 から 18 のいずれか 1 項に記載の出力方法により長さ N の擬似乱数列を出力する出力工程と、

前記入力を受け付けられた伝送信号を、前記出力された長さ N の擬似乱数列を拡散符号として、スペクトラム拡散する拡散工程と、

前記スペクトラム拡散された結果の信号を送信する信号送信工程と、

を備えることを特徴とする送信方法。

【請求項 20】

系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を選択する
選択工程と、

前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を送信するパラメータ送信工程と、

をさらに備え、

前記出力工程は、前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さ N の擬似乱数列を出力する

ことを特徴とする請求項 19 に記載の送信方法。

【請求項 21】

系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を受信するパラメータ受信工程

をさらに備え、

前記出力工程は、前記受信された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さ N の擬似乱数列を出力する

ことを特徴とする請求項 19 に記載の送信方法。

【請求項 22】

信号を受信する信号受信工程と、

請求項 15 から 18 のいずれか 1 項に記載の出力方法により長さ N の擬似乱数列を出力する出力工程と、

前記受信された信号を、前記出力された長さ N の擬似乱数列を拡散符号として、スペクトラム逆拡散する逆拡散工程と、

前記スペクトラム逆拡散された結果の信号を伝送信号として出力する出力工程と、

を備えることを特徴とする受信方法。

【請求項 23】

系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を選択する選択工程と、

前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を送信するパラメータ送信工程と、

をさらに備え、

前記出力工程は、前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメー

タ p_1, p_2, \dots, p_s と、の入力を受け付けて、長さ N の擬似乱数列を出力することを特徴とする請求項 22 に記載の受信方法。

【請求項 24】

系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を受信するパラメータ受信工程と、

をさらに備え、

前記出力工程は、前記受信された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、の入力を受け付けて、長さ N の擬似乱数列を出力することを特徴とする請求項 22 に記載の受信方法。

【請求項 25】

所定の実インパルス定数 r ($-1 < r < 1$) に対するフィルタ方法であって、

チップ長 D の入力信号の入力を受け付ける入力工程と、

前記入力を受け付けられた入力信号を、それぞれ $0, D, 2D, 3D, \dots, (N-1)D$ だけ遅延させた複数の信号を出力する遅延工程と、

前記遅延されて出力された複数の信号のそれぞれを、当該遅延時間が T である場合、 $(-r)^{(N-T)/D}$ 倍して出力する増幅工程と、

前記増幅されて出力された複数の信号の総和を出力する加算工程と、

前記加算されて出力された信号を出力する出力工程と、

を備えることを特徴とするフィルタ方法。

【請求項 26】

コンピュータを、

s ($1 \leq s$) 個の所定の正整数 q_1, q_2, \dots, q_s と、所定の実インパルス定数 r ($-1 < r < 1$) と、に対して、長さ N ($1 \leq N$) の擬似乱数列を出力する擬似乱数列の出力装置であって、

s ($1 \leq s$) 個の実数の系列初期値 Y_1, Y_2, \dots, Y_s ($-1 < Y_1 < 1, -1 < Y_2 < 1, \dots, -1 < Y_s < 1$) と、

s 個の整数パラメータ p_1, p_2, \dots, p_s ($2 \leq p_1, 2 \leq p_2, \dots, 2 \leq p_s$) であって、そのそれぞれについて、前記所定の正整数 q_1, q_2, \dots, q_s に対して、 $q_1 \bmod p_1 \neq 0, q_2 \bmod p_2 \neq 0, \dots, q_s \bmod p_s \neq 0$ が成立する s 個の整数パラメータと、

の入力を受け付ける入力受付部と、

前記所定の実インパルス定数 r と、前記系列初期値 Y_1, Y_2, \dots, Y_s と、前記整数パラメータ p_1, p_2, \dots, p_s と、前記所定の正整数 q_1, q_2, \dots, q_s と、整数 j ($1 \leq j \leq s$), m ($1 \leq m \leq 2N-2$), n ($1 \leq n \leq 2N-1$)と、についての漸化式

【数 9】

$$T_p(\cos \theta) = T(p, \cos \theta) = \cos(p\theta)$$

$$y_j[1] = Y_j$$

$$y_j[m+1] = T(p_j, y_j[m])$$

$$z[n] = \prod_{j=1}^s T(q_j, y_j[n])$$

から、長さ N の擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ であって、

【数 1 0】

$$z'[1] = \sum_{j=1}^N (-r)^j z[j],$$

$$z'[2] = \sum_{j=1}^N (-r)^j z[j+1],$$

\vdots

$$z'[N] = \sum_{j=1}^N (-r)^j z[j+N-1]$$

を満たす擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ を計算する計算部と、

前記擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ を出力する出力部と、

を備える出力装置として機能させることを特徴とするプログラムを記録したコンピュータ読取可能な情報記録媒体。

【請求項 2 7】

前記プログラムは、前記コンピュータにおいて、

前記系列初期値 Y_1, Y_2, \dots, Y_s は、整数 k ($1 \leq k \leq s$)と、整数 m ($1 \leq m \leq N$)と、
に対して

【数 1 1】

$$\begin{aligned}
 y_k[2] &= T(p_k, Y_k) \\
 y_k[m+1] &= T(p_k, y_k[m]) \\
 Y_k &= y_k[N+1] = T(p_k, y_k[N])
 \end{aligned}$$

を満足するように機能させることを特徴とする請求項 26 に記載の情報記録媒体。

【請求項 28】

前記プログラムは、前記コンピュータにおいて、
前記所定の実インパルス定数 r は、

【数 1 2】

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

を満足するように機能させることを特徴とする請求項 26 または 27 に記載の情報記録媒体。

【請求項 29】

前記プログラムは、前記コンピュータにおいて、
前記所定の正整数 q_1, q_2, \dots, q_s は、いずれも 1 である
ように機能させることを特徴とする請求項 26 から 28 のいずれか 1 項に記載
の情報記録媒体。

【請求項 30】

コンピュータを、
伝送信号の入力を受け付ける入力受付部、
請求項 1 から 4 のいずれか 1 項に記載の長さ N の擬似乱数列を出力する出力装
置、
前記入力を受け付けられた伝送信号を、前記出力された長さ N の擬似乱数列を
拡散符号として、スペクトラム拡散する拡散部、および、
前記スペクトラム拡散された結果の信号を送信する信号送信部
として機能させることを特徴とするプログラムを記録したコンピュータ読取可

能な情報記録媒体。

【請求項 3 1】

前記プログラムは、前記コンピュータを、

系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を選択する
選択部、および、

前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S
と、を送信するパラメータ送信部

としてさらに機能させ、

前記出力装置は、前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメー
タ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さ N の擬似乱数列を出力する

ように機能させることを特徴とする請求項 3 0 に記載の情報記録媒体。

【請求項 3 2】

前記プログラムは、前記コンピュータを、

系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を受信する
パラメータ受信部

としてさらに機能させ、

前記出力装置は、前記受信された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメー
タ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さ N の擬似乱数列を出力する

ように機能させることを特徴とする請求項 3 0 に記載の情報記録媒体。

【請求項 3 3】

コンピュータを、

信号を受信する信号受信部、

請求項 1 から 4 のいずれか 1 項に記載の長さ N の擬似乱数列を出力する出力装
置、

前記受信された信号を、前記出力された長さ N の擬似乱数列を拡散符号として
、スペクトラム逆拡散する逆拡散部、および、

前記スペクトラム逆拡散された結果の信号を伝送信号として出力する出力部

として機能させることを特徴とするプログラムを記録したコンピュータ読取可
能な情報記録媒体。

【請求項 3 4】

前記プログラムは、前記コンピュータを、
系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を選択する
選択部、および、
前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S
と、を送信するパラメータ送信部
としてさらに機能させ、
前記出力装置は、前記選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメー
タ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さ N の擬似乱数列を出力する
ように機能させることを特徴とする請求項 3 3 に記載の情報記録媒体。

【請求項 3 5】

前記プログラムは、前記コンピュータを、
系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を受信する
パラメータ受信部
としてさらに機能させ、
前記出力装置は、前記受信された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメー
タ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さ N の擬似乱数列を出力する
ように機能させることを特徴とする請求項 3 3 に記載の情報記録媒体。

【請求項 3 6】

コンピュータ、DSP (Digital Signal Processor)、もしくは、FPGA (Field Programmable Gate Array) を、
所定の実インパルス定数 r ($-1 < r < 1$) に対するフィルタ装置であって、
チップ長 D の入力信号の入力を受け付ける入力端子と、
前記入力を受け付けられた入力信号を、それぞれ $0, D, 2D, 3D, \dots, (N-1)D$ だ
け遅延させた複数の信号を出力する遅延部と、
前記遅延されて出力された複数の信号のそれぞれを、当該遅延時間が T である
場合、 $(-r)^{(N-T)/D}$ 倍して出力する増幅部と、
前記増幅されて出力された複数の信号の総和を出力する加算部と、
前記加算されて出力された信号を出力する出力端子と、

を備えるフィルタ装置として機能させることを特徴とするプログラムを記録したコンピュータ読取可能な情報記録媒体。

【請求項 3 7】

前記情報記録媒体は、コンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、または、半導体メモリであることを特徴とする請求項 2 6 から 3 6 のいずれか 1 項に記載の情報記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置、擬似乱数列の出力方法、送信方法、受信方法、フィルタ方法、ならびに、情報記録媒体に関する。

【 0 0 0 2 】

特に、衛星通信、固定通信、携帯電話や P H S (Personal Handyphone System) などの陸上移動通信や G P S (Global Positioning System) などの測距分野で用いることができるスペクトラム拡散通信の非同期 C D M A (Code Division Multiple Access ; 符号分割多元接続) 方式の拡散符号として使用できる擬似乱数列を出力するのに好適な出力装置、出力方法と、これを用いた送信装置、受信装置、通信システム、フィルタ装置、送信方法、受信方法、フィルタ方法、ならびに、これらを実現するためのプログラムを記録したコンピュータ読取可能な情報記録媒体に関する。

【 0 0 0 3 】

【従来の技術】

従来から、スペクトラム拡散通信、符号分割多重通信を実現する拡散符号として、線形帰還シフトレジスタ (Linear Feedback Shift Register ; L F S R) によって作られる、M 系列、嵩符号、ゴールド系列等が提案されている。これらの拡散符号系列には、以下の 2 つの特徴がある。

【 0 0 0 4 】

第1に、同じ符号同士の相関（自己相関）に一つのピークを持ち、異なる符号同士の相関（相互相関）は0である。これは、白色雑音（white noise）の性質に極めて類似している。

【0005】

第2に、符号集合に含まれる異なる2つの拡散符号を選択した場合、いずれを選択してもその相互相関が0に近くなるように符号集合を構成した場合、符号集合に含まれる符号の数が、符号長 N に対して $O(N)$ しかない。このため、符号の種類が少ない。

【0006】

一方、古くからTDMA（Time Division Multiple Access；時分割多元接続）やFDMA（Frequency Division Multiple Access；周波数分割多元接続）も知られている。非同期CDMA通信システムは、これらと異なり、信号の同期を積極的にとらなくとも、用いられる符号の相関特性を利用して、復号ができるという特徴を有する。このため、秘話性、秘匿性、耐干渉・妨害性、などに優れる。

【0007】

現在非同期CDMA通信システムは、実用化が進められており、IMT-2000（International Mobile Telecommunication 2000）という次世代無線通信のITU（International Telecommunication Union）標準規格として採用が決まっている。

【0008】

近年の研究により、非同期CDMA通信システムでは、符号間干渉ノイズの分散 σ が、システムの性能を決めることがわかっている。この分散 σ は、ゴールド符号や嵩符号などの擬似白色雑音を拡散符号として用いる場合に、同時接続ユーザー数を K とし、符号長を N とすると、漸近的に $\sigma = (K-1)/3N$ であることが、たとえば以下の文献に開示されている。

M. B. Pursley, 「Performance Evaluation for Phased-Coded Spread-Spectrum Multiple-Access Communication-Part I: System Analysis」 (IEEE Trans. Communications, vol.25 (1977) pp.795-799.)

【0009】

ここで、「漸近的」とは、ユーザー数 K と、符号長 N とを大きくとった場合、という意味である。

【0010】

従来、非同期CDMA通信システムの性能の理論的限界は、この $\sigma = (K-1)/3N$ であると考えられていた。しかしながら、このような漸近的關係が成立するのは、拡散符号が、擬似白色雑音であるということに起因することもわかっていた。

【0011】

したがって、拡散符号が擬似白色雑音でない場合、すなわち、異なる符号の間にいくらかの相関がある場合には、性能の理論的限界が向上する可能性もあった。

【0012】

最近になって、拡散符号が擬似白色雑音である場合に比べて符号間干渉ノイズの分散 σ が減少するような自己相関関数を持つ拡散符号の存在が発見された。すなわち、自己相関関数が符号のシフト l に対して、[数13]のように指数関数的に減少する場合は、その干渉ノイズの分散 σ は、擬似白色雑音の場合よりも小さくなる。

【0013】

【数13】

$$C(l) \approx Const. \times (-r)^l \quad (-1 < r < 1)$$

【0014】

特に、実インパルス定数 r が[数14]を満たす場合、[数15]のような最適相関関数の形をとる。

【0015】

【数14】

$$r = 2 - \sqrt{3}$$

【0016】

【数15】

$$\sigma_{optimal} = \frac{\sqrt{3}(K-1)}{6N}$$

【0017】

これは、同一ビット誤り率での同時接続ユーザー数Kが、擬似白色雑音を拡散符号として用いた場合の非同期CDMA通信システムのユーザー数の理論限界より15パーセントも増えるということである。この点については、以下の文献に開示されている。

G. Mazzini, R. Rovatti, and G. Setti 「Interference Minimization by Auto-Correlation Shaping in Asynchronous DS-CDMA Systems: Chaos-Based Spreading is Nearly Optimal」 (Electron. Lett. (1999) vol.35, pp.1054-1055)

【0018】

また、同文献では、部分的傾きが極めて大きい多段線形写像を用いてカオス敵拡散符号を構成することにより、【数13】を満足する相関関数を近似的に模式できることが示されている。

【0019】

【発明が解決しようとする課題】

しかしながら、このような拡散系列をDSP (Digital Signal Processor) などを用いて実際に生成して携帯電話などで利用するためには、高速性と低消費電力が必要となるため、以下のような課題が発生していた。

【0020】

第1に、拡散符号が極めて大きな傾きの多段線形写像で構成されているため、DSPやコンピュータなどで計算を行うと、桁落ちが大きくなり、正確な結果が得られない、という問題があった。このため、物理的な回路や装置を構成して、拡散符号を生成することは難しい、という課題があった。

【0021】

第2に、相関関数の減衰の様子を決定するパラメータを、任意の r ($-1 < r < 1$) に対して自由自在に調整することができない、という課題があった。

【0022】

第3に、上記文献では、最適相関関数に近い相関関数を持つ多段線形写像の種類は少ないことが示されている。しかしながら、CDMA通信システムを実現するためには、できるかぎり多種類の符号があった方がよい。このため、上記文献に開示される手法を用いるのでは、CDMA通信システムを現実構成することは難しかった。

【0023】

第4に、線形シフトレジスタを用いて生成した拡散符号では、符号長 N に対して、相関特性の良い符号の種類は、 $O(N)$ しかない。本来の符号の種類は、2のべき乗に比例する数 $O(2^N)$ だけあるのに対して、これでは極めて少ない。このため、ユーザー数の増大に対応することが難しい。

【0024】

第5に、鍵空間が狭いため、解読に必要な手間が少ない。このため、通信セキュリティが弱くなってしまうという問題が生ずる。

【0025】

これらの問題については、上記文献に開示される技術では、改善がなされていない。

【0026】

したがって、このような課題を解決しつつ、非同期CDMA通信システムに適した擬似乱数列(PN(Pseudo Noise; 擬似雑音)系列ともいう。)からなる拡散符号の生成技術が強く望まれている。

【0027】

本発明は、非同期CDMA通信システムに適した擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置、擬似乱数列の出力方法、送信方法、受信方法、フィルタ方法、ならびに、これらを実現するためのプログラムを記録したコンピュータ読取可能な情報記録媒体を提供することを目的とする。

【0028】

【課題を解決するための手段】

以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【0 0 2 9】

本発明の第 1 の観点に係る擬似乱数列の出力装置は、 s ($1 \leq s$) 個の所定の正整数 q_1, q_2, \dots, q_s と、所定の実インパルス定数 r ($-1 < r < 1$) と、に対して、長さ N ($1 \leq N$) の擬似乱数列を出力し、入力受付部と、計算部と、出力部と、を備えるように構成する。

【0 0 3 0】

ここで、入力受付部は、 s ($1 \leq s$) 個の実数の系列初期値 Y_1, Y_2, \dots, Y_s ($-1 < Y_1 < 1, -1 < Y_2 < 1, \dots, -1 < Y_s < 1$) と、 s 個の整数パラメータ p_1, p_2, \dots, p_s ($2 \leq p_1, 2 \leq p_2, \dots, 2 \leq p_s$) であって、そのそれぞれについて、所定の正整数 q_1, q_2, \dots, q_s に対して、 $q_1 \bmod p_1 \neq 0, q_2 \bmod p_2 \neq 0, \dots, q_s \bmod p_s \neq 0$ が成立する s 個の整数パラメータと、の入力を受け付ける。

【0 0 3 1】

一方、計算部は、所定の実インパルス定数 r と、系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、所定の正整数 q_1, q_2, \dots, q_s と、整数 j ($1 \leq j \leq s$), m ($1 \leq m \leq 2N-2$), n ($1 \leq n \leq 2N-1$) と、についての漸化式

【0 0 3 2】

【数 1 6】

$$T_p(\cos \theta) = T(p, \cos \theta) = \cos(p\theta)$$

$$y_j[1] = Y_j$$

$$y_j[m+1] = T(p_j, y_j[m])$$

$$z[n] = \prod_{j=1}^s T(q_j, y_j[n])$$

から、長さ N の擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ であって、

【0 0 3 3】

【数 1 7】

$$\begin{aligned}
 z'[1] &= \sum_{j=1}^N (-r)^j z[j], \\
 z'[2] &= \sum_{j=1}^N (-r)^j z[j+1], \\
 &\vdots \\
 z'[N] &= \sum_{j=1}^N (-r)^j z[j+N-1]
 \end{aligned}$$

を満たす擬似乱数列 $z'[1]$, $z'[2]$, ..., $z'[N]$ を計算する。

【0 0 3 4】

さらに、出力部は、擬似乱数列 $z'[1]$, $z'[2]$, ..., $z'[N]$ を出力する。

【0 0 3 5】

また、本発明の疑似乱数列の出力装置において、系列初期値 Y_1, Y_2, \dots, Y_s は、整数 k ($1 \leq k \leq s$) と、整数 m ($1 \leq m \leq N$) と、に対して

【0 0 3 6】

【数 1 8】

$$\begin{aligned}
 y_k[2] &= T(p_k, Y_k) \\
 y_k[m+1] &= T(p_k, y_k[m]) \\
 Y_k &= y_k[N+1] = T(p_k, y_k[N])
 \end{aligned}$$

を満足するように構成することができる。

【0 0 3 7】

また、本発明の疑似乱数列の出力装置において、所定の実インパルス定数 r は

【0 0 3 8】

【数 1 9】

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

を満足するように構成することができる。

【0039】

また、本発明の疑似乱数列の出力装置において、所定の正整数 q_1, q_2, \dots, q_s は、いずれも1であるように構成することができる。

【0040】

本発明の第2の観点に係る送信装置は、入力受付部と、上記の疑似乱数列の出力装置と、拡散部と、信号送信部と、を備えるように構成する。

【0041】

ここで、入力受付部は、伝送信号の入力を受け付ける。

【0042】

一方、出力装置は、長さ N の疑似乱数列を出力する。

【0043】

さらに、拡散部は、入力を受け付けられた伝送信号を、出力された長さ N の疑似乱数列を拡散符号として、スペクトラム拡散する。

【0044】

そして、信号送信部は、スペクトラム拡散された結果の信号を送信する。

【0045】

また、本発明の送信装置は、選択部と、パラメータ送信部と、をさらに備えるように構成することができる。

【0046】

ここで、選択部は、系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を選択する。

【0047】

一方、パラメータ送信部は、選択された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を送信する。

【0048】

さらに、出力装置は、選択された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、の入力を受け付けて、長さ N の疑似乱数列を出力する。

【0049】

また、本発明の送信装置は、パラメータ受信部をさらに備えるように構成することができる。

【0050】

ここで、パラメータ受信部は、系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を受信する。

【0051】

一方、出力装置は、受信された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さ N の疑似乱数列を出力する。

【0052】

本発明の第3の観点に係る受信装置は、信号受信部と、上記の疑似乱数列の出力装置と、逆拡散部と、出力部と、を備えるように構成する。

【0053】

ここで、信号受信部は、信号を受信する。

【0054】

一方、出力装置は、長さ N の疑似乱数列を出力する。

【0055】

さらに、逆拡散部は、受信された信号を、出力された長さ N の疑似乱数列を拡散符号として、スペクトラム逆拡散する。

【0056】

そして、出力部は、スペクトラム逆拡散された結果の信号を伝送信号として出力する。

【0057】

また、本発明の受信装置は、選択部と、パラメータ送信部と、をさらに備えるように構成することができる。

【0058】

ここで、選択部は、系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を選択する。

【0059】

一方、パラメータ送信部は、選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パ

ラメータ p_1, p_2, \dots, p_s と、を送信する。

【0 0 6 0】

さらに、出力装置は、選択された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、の入力を受け付けて、長さ N の擬似乱数列を出力する。

【0 0 6 1】

また、本発明の受信装置は、パラメータ受信部をさらに備えるように構成することができる。

【0 0 6 2】

ここで、パラメータ受信部は、系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を受信する。

【0 0 6 3】

一方、出力装置は、受信された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、の入力を受け付けて、長さ N の擬似乱数列を出力する。

【0 0 6 4】

本発明の第 4 の観点に係る通信システムは、上記の送信装置と、上記の受信装置と、を備えるように構成する。

【0 0 6 5】

ここで、受信装置は、送信装置から送信された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を受信する。

【0 0 6 6】

また、受信装置は、送信装置から送信された信号を受信する。

【0 0 6 7】

本発明の第 5 の観点に係る通信システムは、上記の送信装置と、上記の受信装置と、を備えるように構成する。

【0 0 6 8】

ここで、送信装置は、受信装置から送信された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、を受信する。

【0 0 6 9】

また、受信装置は、送信装置から送信された信号を受信する。

【0 0 7 0】

本発明の第6の観点に係るフィルタ装置は、所定の実インパルス定数 r ($-1 < r < 1$)に対してフィルタ処理を行い、入力端子と、遅延部と、増幅部と、加算部と、出力端子と、を備えるように構成する。

【0 0 7 1】

ここで、入力端子は、チップ長 D の入力信号の入力を受け付ける。

【0 0 7 2】

一方、遅延部は、入力を受け付けられた入力信号を、それぞれ 0 、 D 、 $2D$ 、 $3D$ 、 \dots 、 $(N-1)D$ だけ遅延させた複数の信号を出力する。

【0 0 7 3】

さらに、増幅部は、遅延されて出力された複数の信号のそれぞれを、当該遅延時間が T である場合、 $(-r)^{(N-T)/D}$ 倍して出力する。

【0 0 7 4】

そして、加算部は、増幅されて出力された複数の信号の総和を出力する。

【0 0 7 5】

一方、出力端子は、加算されて出力された信号を出力する。

【0 0 7 6】

また、本発明のフィルタ装置の遅延部、増幅部、および、加算部は、ASIC (Application Specific Integrated Circuit)、DSP (Digital Signal Processor)、もしくは、FPGA (Field Programmable Gate Array) によって構成することができる。

【0 0 7 7】

本発明の第7の観点に係る擬似乱数列の出力方法は、 s ($1 \leq s$)個の所定の正整数 q_1, q_2, \dots, q_s と、所定の実インパルス定数 r ($-1 < r < 1$)と、に対して、長さ N ($1 \leq N$)の擬似乱数列を出力し、入力受付工程と、計算工程と、出力工程と、を備えるように構成する。

【0 0 7 8】

ここで、入力受付工程では、 s ($1 \leq s$)個の実数の系列初期値 Y_1, Y_2, \dots, Y_s ($-1 < Y_1 < 1, -1 < Y_2 < 1, \dots, -1 < Y_s < 1$)と、

s 個の整数パラメータ p_1, p_2, \dots, p_s ($2 \leq p_1, 2 \leq p_2, \dots, 2 \leq p_s$)であって、そのそれぞれについて、所定の正整数 q_1, q_2, \dots, q_s に対して、 $q_1 \bmod p_1 \neq 0$, $q_2 \bmod p_2 \neq 0, \dots, q_s \bmod p_s \neq 0$ が成立する s 個の整数パラメータと、の入力を受け付ける。

【0079】

一方、計算工程では、所定の実インパルス定数 r と、系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、所定の正整数 q_1, q_2, \dots, q_s と、整数 j ($1 \leq j \leq s$), m ($1 \leq m \leq 2N-2$), n ($1 \leq n \leq 2N-1$) と、についての漸化式 [数16] から、長さ N の擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ であって、[数17] を満たす擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ を計算する。

【0080】

さらに、出力工程では、擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ を出力する。

【0081】

また、本発明の疑似乱数列の出力方法において、系列初期値 Y_1, Y_2, \dots, Y_s は、整数 k ($1 \leq k \leq s$) に対して [数18] を満足するように構成することができる。

【0082】

また、本発明の疑似乱数列の出力方法において、所定の実インパルス定数 r は、[数19] を満足するように構成することができる。

【0083】

また、本発明の疑似乱数列の出力方法において、所定の正整数 q_1, q_2, \dots, q_s は、いずれも 1 であるように構成することができる。

【0084】

本発明の第8の観点に係る本発明の送信方法は、入力受付工程と、出力工程と、拡散工程と、信号送信工程と、を備えるように構成する。

【0085】

ここで、入力受付工程では、伝送信号の入力を受け付ける。

【0086】

一方、出力工程では、上記の疑似乱数列の出力方法により長さ N の疑似乱数列

を出力する。

【0087】

さらに、拡散工程では、入力を受け付けられた伝送信号を、出力された長さNの擬似乱数列を拡散符号として、スペクトラム拡散する。

【0088】

そして、信号送信工程では、スペクトラム拡散された結果の信号を送信する。

【0089】

また、本発明の送信方法は、選択工程と、パラメータ送信工程と、をさらに備えるように構成することができる。

【0090】

ここで、選択工程では、系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を選択する。

【0091】

一方、パラメータ送信工程では、選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を送信する。

【0092】

さらに、出力工程では、選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さNの擬似乱数列を出力する。

【0093】

また、本発明の送信方法は、パラメータ受信工程をさらに備えるように構成することができる。

【0094】

ここで、パラメータ受信工程では、系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を受信する。

【0095】

一方、出力工程では、受信された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さNの擬似乱数列を出力する。

【0096】

本発明の第9の観点に係る受信方法は、信号受信工程と、出力工程と逆拡散工

程と、出力工程と、を備えるように構成する。

【0097】

ここで、信号受信工程では、信号を受信する。

【0098】

一方、出力工程では、上記の疑似乱数列の出力方法により長さNの疑似乱数列を出力する。

【0099】

さらに、逆拡散工程では、受信された信号を、出力された長さNの疑似乱数列を拡散符号として、スペクトラム逆拡散する。

【0100】

そして、出力工程では、スペクトラム逆拡散された結果の信号を伝送信号として出力する。

【0101】

また、本発明の受信方法は、選択工程と、パラメータ送信工程と、をさらに備えるように構成することができる。

【0102】

ここで、選択工程では、系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を選択する。

【0103】

一方、パラメータ送信工程では、選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、を送信する。

【0104】

さらに、出力工程では、選択された系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメータ p_1, p_2, \dots, p_S と、の入力を受け付けて、長さNの疑似乱数列を出力する。

【0105】

また、本発明の受信方法は、パラメータ受信工程をさらに備えるように構成することができる。

【0106】

ここで、パラメータ受信工程では、系列初期値 Y_1, Y_2, \dots, Y_S と、整数パラメ

ータ p_1, p_2, \dots, p_s と、を受信する。

【0107】

一方、出力工程では、受信された系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、の入力を受け付けて、長さ N の擬似乱数列を出力する。

【0108】

本発明の第9に係るフィルタ方法は、所定の実インパルス定数 r ($-1 < r < 1$) に対してフィルタ処理を行い、入力工程と、遅延工程と、増幅工程と、加算工程と、出力工程と、を備えるように構成する。

【0109】

ここで、入力工程では、チップ長 D の入力信号の入力を受け付ける。

【0110】

一方、遅延工程では、入力を受け付けられた入力信号を、それぞれ $0, D, 2D, 3D, \dots, (N-1)D$ だけ遅延させた複数の信号を出力する。

【0111】

さらに、増幅工程では、遅延されて出力された複数の信号のそれぞれを、当該遅延時間が T である場合、 $(-r)^{(N-T)/D}$ 倍して出力する。

【0112】

そして、加算工程では、増幅されて出力された複数の信号の総和を出力する。

【0113】

一方、出力工程では、加算されて出力された信号を出力する。

【0114】

なお、上記発明において、それぞれの系列初期値 Y_k ($1 \leq k \leq s$) は、カオス写像 $T(p_k, \cdot)$ による力学系

$$X_{n+1} = T(p_k, X_n)$$

の周期 N の周期点であるように構成することができる。この性質を使うことにより、重複した計算を省略して高速な擬似乱数生成ができるようになる。

【0115】

本発明の擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置にて実行される処理と、擬似乱数列の出力方法、送信方法、受信方法、な

らびに、フィルタ方法と、を実現するプログラムを、コンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、半導体メモリなどのコンピュータ読取可能な情報記録媒体に記録することができる。

【0116】

本発明の情報記録媒体に記録されたプログラムを、記憶装置、計算装置、出力装置、通信装置などを備える汎用コンピュータ、携帯電話機、PHS装置、ゲーム装置などの携帯端末、並列計算機などの情報処理装置、DSP (Digital Signal Processor)、FPGA (Field Programmable Gate Array) などで実行することにより、上記の擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置にて実行される処理と、擬似乱数列の出力方法、送信方法、受信方法、ならびに、フィルタ方法を実現することができる。

【0117】

また、情報処理装置とは独立して、本発明のプログラムを記録した情報記録媒体を配布、販売することができる。

【0118】

【発明の実施の形態】

以下に本発明の実施形態を説明する。なお、以下にあげる実施形態は、説明のためのものであり、本発明の範囲を制限するものではない。したがって、当業者であれば、これらの各要素または全要素を、これと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も、本発明の範囲に含まれる。

【0119】

(第1の実施の形態)

図1は、本発明の第1の実施の形態に係る擬似乱数列の出力装置の概要構成を示す模式図(データフロー図)である。以下、本図を参照して説明する。

【0120】

本実施形態に係る擬似乱数列の出力装置101は、 s ($1 \leq s$)個の所定の正整数 q_1, q_2, \dots, q_s と、所定の実インパルス定数 r ($-1 < r < 1$)と、に対して、長さ N

($1 \leq N$)の擬似乱数列を出力し、入力受付部 1 0 2 と、計算部 1 0 3 と、出力部 1 0 4 と、を備える。

【0 1 2 1】

ここで、入力受付部 1 0 2 は、以下の系列初期値と整数パラメータの入力を受け付ける。

・ s 個の実数の系列初期値 Y_1, Y_2, \dots, Y_s 。ただし、 $-1 < Y_1 < 1, -1 < Y_2 < 1, \dots, -1 < Y_s < 1$ 。

・ s 個の整数パラメータ p_1, p_2, \dots, p_s 。ただし、 $2 \leq p_1, 2 \leq p_2, \dots, 2 \leq p_s$ である。また、そのそれぞれについて、所定の正整数 $q_1 \bmod p_1 \neq 0, q_2 \bmod p_2 \neq 0, \dots, q_s \bmod p_s \neq 0$ が成立する。

【0 1 2 2】

計算部 1 0 3 は、所定の実インパルス定数 r と、入力を受け付けられた系列初期値 Y_1, Y_2, \dots, Y_s と、整数パラメータ p_1, p_2, \dots, p_s と、所定の正整数 q_1, q_2, \dots, q_s と、整数 j ($1 \leq j \leq s$), m ($1 \leq m \leq 2N-2$), n ($1 \leq n \leq 2N-1$) と、についての漸化式 [数 1 6] から、長さ N の擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ であって、[数 1 7] を満たす擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ を計算する。

【0 1 2 3】

出力部 1 0 4 は、計算された擬似乱数列 $z'[1], z'[2], \dots, z'[N]$ を出力する。

【0 1 2 4】

図 2 は、計算部 1 0 3 で用いられるチェビシェフ多項式を表したグラフである。チェビシェフ多項式は、整数 a を次数とすると、

$$T(a, \cos \theta) = \cos(a \theta)$$

のように、余弦関数の加法定理により定義することができる。一方、以下のように、有理多項式で直接表現することもできる。

$$T(0, x) = 1$$

$$T(1, x) = x$$

$$T(2, x) = 2x^2 - 1$$

$$T(3, x) = 4x^3 - 3x$$

【0 1 2 5】

チェビシェフ多項式 $y = T(a, x)$ は、いずれも、开区間 $-1 < x < 1$ を开区間 $-1 < y < 1$ に写像する有理写像である。

【0 1 2 6】

本図には、次数 2 から 5 のチェビシェフ多項式が、 $y = T(2, x)$, $y = T(3, x)$, $y = T(4, x)$, $y = T(5, x)$ の形式でグラフ表示されている。横軸が x 軸、縦軸が y 軸である。

【0 1 2 7】

計算部 1 0 3 の計算は、コンピュータによる多項式演算により実現することができるほか、加減算回路と乗算回路の組合せによっても実現できる。また、所定の精度保証をした浮動小数点演算で実現してもよいし、有理数による演算により実現することもできる。この点については後述する。

【0 1 2 8】

また、入力受付部 1 0 2 における系列初期値および整数パラメータの入力の受付や、出力部 1 0 4 における出力は、コンピュータの場合には R A M (Random Access Memory) や C P U (Central Processing Unit; 中央処理ユニット) 内のレジスタを介して行うことができ、電子回路の場合には、ラッチなどを用いて実現することができる。

【0 1 2 9】

上記の漸化式を見れば明らかなように、 $z'[1]$, $z'[2]$, ..., $z'[N]$ をそれぞれ求めるための計算は互いに独立しているため、並列度最大 N で並列に計算を行うことができる。また、漸化式で記述されているため、ループによる繰り返し演算によっても容易に計算を行うことができる。

【0 1 3 0】

本実施形態により出力される長さ N の擬似乱数列の相関関数が、上記の最適相関関数となることは、エルゴード理論において展開されるルベグスペクトラム (Lebesgue Spectrum) の理論に基づく。本理論については、以下の文献に開示されている。

V. I. Arnold and A. Avez [Ergodic Problems of Classical Mechanics]

(W. A. Benjamin, New York, 1968)

【0 1 3 1】

以下、ルベークスペクトラムの理論を説明する。

【0 1 3 2】

今、 $X_{n+1}=F(X_n)$ という力学系から生成された系列 X_1, X_2, \dots が、その力学系を定義する領域 M 上の極限密度分布関数（不変測度） $\rho(x)dx$ に対して、エルゴード性を持つとする。

【0 1 3 3】

すると、この不変測度に関する内積

$$\langle u, v \rangle = \int_M u(x)v(x) \rho(x)dx$$

から、自然にノルム演算 $\| \cdot \|$ が

$$\|v\|^2 = \langle v, v \rangle$$

のように定義されるヒルベルト空間 L_2 を考えることができる。

【0 1 3 4】

上記文献によれば、この L_2 空間に、ある力学系に依存する特殊な性質を満足する正規直交基底 [数 2 0] が一意的に存在する。これをルベークスペクトラムと呼ぶ。

【0 1 3 5】

【数 2 0】

$$\{\phi_{\lambda,j}\}_{\lambda \in \Lambda, j \in \mathcal{J}}$$

【0 1 3 6】

ここで、 λ は、このルベークスペクトラムの各クラスをラベル付けするものであり、 j は、その各クラスの関数を指し示すラベルで加算無限個ある 0 以上の整数に対応する。

【0 1 3 7】

この定義から、ルベークスペクトラムは、無限個の関数からなる正規直交関数系であることがわかる。特に、ラベル λ のとりうる種類の数（ Λ の cardinality）が無限の場合、このルベークスペクトラムを無限ルベークスペクトラムと呼ぶ

。また、このルベークスペクトラムが、正規直交基底だけではなく、 L_2 空間において完全正規直交基底である場合には、このルベークスペクトラムを完全ルベークスペクトラムと呼ぶ。

【0138】

さて、上述のルベークスペクトラムの持つ特殊な性質とは、[数21]を満足することである。

【0139】

【数21】

$$\phi_{\lambda,j} \circ F(x) = \phi_{\lambda,j+1}(x) \\ (\text{for } \forall \lambda \in \Lambda, \forall j \in \mathcal{J})$$

【0140】

即ち、もし、以下の関数[数22]が与えられれば、クラス λ の他のルベークスペクトラム関数[数23]は、すべて、力学系を定義する写像 $F(\cdot)$ を繰り返して、適用することにより得ることができる。

【0141】

【数22】

$$\phi_{\lambda,0}$$

【0142】

【数23】

$$\{\phi_{\lambda,j}\}_{j \geq 1}$$

【0143】

また、ルベークスペクトラムが正規直交系を成すという仮定により、これらの各関数[数24]は、同一のクラスの任意の他の関数[数25]および、任意の他のクラスの任意の関数[数26]と直交する。

【0144】

【数 2 4】

$$\phi_{\lambda,j}$$

【0 1 4 5】

【数 2 5】

$$\phi_{\lambda,j'}$$

【0 1 4 6】

【数 2 6】

$$\phi_{\lambda',j''}$$

【0 1 4 7】

完全なルベーグスペクトラムを持つエルゴード力学系として、後で述べる 2 次以上のチェビシェフ多項式で与えられるチェビシェフカオス力学系がある。チェビシェフカオス力学系については、以下の文献に開示されている。

R. L. Adler, T. J. Rivlin 「Proc. Am. Math. Soc. 15」 (1964, p 794)

【0 1 4 8】

今、 L_2 のある関数 $B(x)$ が、【数 2 7】 のようにルベーグスペクトラムで展開できるとする。

【0 1 4 9】

【数 2 7】

$$B(x) = \sum_{j=1}^N a_{\lambda,j} \phi_{\lambda,j}(x)$$

【0 1 5 0】

この場合、相関関数【数 2 8】は、ルベーグスペクトラムの直交性から、【数 2 9】のように、ルベーグスペクトラム展開係数により与えられる。

【0 1 5 1】

【数 2 8】

$$\langle B(x), B(F^l(x)) \rangle \equiv \langle B_0, B_l \rangle$$

【0 1 5 2】

【数 2 9】

$$\langle B_0, B_l \rangle = \sum_{m=l}^{\infty} a_{\lambda, m} a_{\lambda, m-l}$$

【0 1 5 3】

なお、この相関関数は、エルゴード性により、時間平均 [数 3 0] に等しい。

【0 1 5 4】

【数 3 0】

$$\overline{B(x)B(F^l(x))} = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N B(X_n)B(X_{n+l})$$

【0 1 5 5】

各 X_n は、漸化式 $X_{n+1} = F(X_n)$ により生成され、この時間平均が空間平均に等しいというエルゴード等式は、 M 上の測度 0 の例外的初期値 X_1 を除いて成立する。

【0 1 5 6】

今、ここで、[数 3 1] と仮定する。

【0 1 5 7】

【数 3 1】

$$a_{\lambda, m} = C(-r)^m \quad (m = 0, 1, \dots)$$

【0 1 5 8】

これを、上の相関関数を与える式に代入すると、[数 3 2] が得られ、相関関数は、[数 3 3] のように、指数関数的に減少する。

【0 1 5 9】

【数 3 2】

$$\langle B_0, B_l \rangle = C^2(-r)^l \frac{1 - r^{2N}}{1 - r^2}$$

【0 1 6 0】

【数 3 3】

$$C(l) \equiv \langle B_0, B_l \rangle = C'(-r)^l \quad (N \rightarrow \infty)$$

【0 1 6 1】

このように、符号シフト量 l に関して、 $(-r)^l$ の形で指数関数的にダンプする相関関数を持つ系列を、任意の r ($-1 < r < 1$) に対して、自由自在に、作ることができる。

【0 1 6 2】

特に、Mazziniが発見したように、ランダム符号（ゴールド符号、嵩符号も含む）を拡散系列とした時よりも、同一ビット誤り率下で、【数 1 4】の場合、15パーセント理論的ユーザー数を増やすことができる。

【0 1 6 3】

干渉ノイズの分散が、【数 1 5】となるような拡散系列は、その相関関数の漸近的振る舞いが、【数 1 3】、【数 1 4】のようになればよい。したがって、ルベグスペクトラムを持つエルゴード力学系と、そのルベグスペクトラム関数により定義される上述の $B(x)$ で、【数 3 4】のように設計されるフィルタを用意すれば十分である。

【0 1 6 4】

【数 3 4】

$$a_{\lambda, m} = C(-r)^m, r = 2 - \sqrt{3} \quad (m = 0, 1, \dots)$$

【0 1 6 5】

さて、ここで問題となるのは、どのようにすれば、エルゴード力学系 $F(x)$ とルベグスペクトラム【数 2 0】とを実現容易な形で構成できるかということであ

る。以下では、チェビシェフ写像による構成について説明する。

【0166】

今、2次以上のチェビシェフ多項式 $T_p(x)$ ($p \geq 2$)を考える。このチェビシェフ多項式は、上述のように、 $T_p(\cos \theta) = \cos(p\theta)$ のように定義され、それぞれの p の値に対して、閉区間 $M=[-1,1]$ 上の分布関数 [数35] の下で、[数36] のように直交することが知られている。

【0167】

【数35】

$$\rho(x)dx = \frac{dx}{\pi\sqrt{1-x^2}}$$

【0168】

【数36】

$$\int_M T_p(x)T_q(x)\rho(x)dx = 0 \quad (\text{for } q \neq p)$$

【0169】

これらのチェビシェフ多項式と分布関数により、ヒルベルト空間 L_2 を構成することができる。この場合、チェビシェフ多項式は、ヒルベルト空間 L_2 における完全性を持つ直交基底となる。

【0170】

また、上述の文献には、2つ以上のチェビシェフ写像で与えられる力学系が、エルゴード性を有するほか、これよりも強い混合性という性質を持つことが開示されている。この場合のエルゴード的な不変測度は、上述の直交性を定義する密度関数 $\rho(x)$ により与えられる。

【0171】

これらの性質から、今、[数37] のように関数系 $\phi_{q,j}(x)$ を定義する。

【0172】

【数 3 7】

$$\phi_{q,j}(x) = T_{qp^j}(x) \quad (j \geq 0, q(\bmod p) \neq 0)$$

【0 1 7 3】

すると、チェビシェフ多項式自身の直交性と、関係式 [数 3 8] とから、関数系 $\phi_{q,j}(x)$ はルベークスペクトラムであることがわかる。

【0 1 7 4】

【数 3 8】

$$\begin{aligned} \phi_{q,j} \circ T_p(x) \\ &= T_{qp^j} \circ T_p(x) \\ &= T_{qp^{j+1}}(x) \\ &= \phi_{q,j+1}(x) \end{aligned}$$

【0 1 7 5】

したがって、[数 3 9] のようにフィルタを設計すれば、上述のルベークスペクトラム理論の相関関数の明示解により、相関関数 [数 1 3] を持つ非同期 CDMA 通信システム用の拡散符号を構成することができる。これは、上述のように、Mazzini の理論により示されたものであり、通常のランダム符号を基礎とする非同期 CDMA のある一定のビット誤り率のもとでのユーザー数を、15 パーセント増加することができる。

【0 1 7 6】

【数 3 9】

$$\begin{aligned} B(x) &= \sum_{j=1}^N (-r)^j \phi_{q,j}(x) \\ &= \sum_{j=1}^N (-r)^j T_{qp^j}(x) \end{aligned}$$

【0 1 7 7】

ここで、[数 4 0] [数 4 1] が成立し、任意の整数 m ($0 \leq m \leq N-1$) に対して

[数 4 2] [数 4 3] であることに着目する。

【0 1 7 8】

【数 4 0】

$$\begin{aligned} B(X_1) &= \sum_{j=1}^N (-r)^j \phi_{q,j}(X_1) \\ &= \sum_{j=1}^N (-r)^j T_{qp^j}(X_1) \end{aligned}$$

【0 1 7 9】

【数 4 1】

$$B(X_1) = \sum_{j=1}^N (-r)^j T_q(X_{1+j})$$

【0 1 8 0】

【数 4 2】

$$\begin{aligned} B(X_m) &= \sum_{j=1}^N (-r)^j \phi_{q,j}(X_m) \\ &= \sum_{j=1}^N (-r)^j T_{qp^{j+m-1}}(X_1) \end{aligned}$$

【0 1 8 1】

【数 4 3】

$$B(X_m) = \sum_{j=1}^N (-r)^j T_q(X_{m+j})$$

【0 1 8 2】

この関数 $B(X)$ は、 $q=1$ の場合、 $T_q(x) = x$ となり、[数 4 4] が成立する。

【0 1 8 3】

【数 4 4】

$$B(X_m) = \sum_{j=1}^N (-r)^j X_{m+j}$$

【0 1 8 4】

これは、系列 X_{m+1} , X_{m+2} , ..., X_{m+j} , ..., X_{m+N-1} , X_{m+N} ($0 \leq m \leq N-1$)を、それぞれ、 $(-r)^j$ に与えられる定数により定数倍した結果の和をとる操作を意味する。

【0 1 8 5】

これは、デジタル信号処理の基本フィルタの一つである F I R フィルタ (Finite Impulse Response Filter) の操作に他ならない。

【0 1 8 6】

よって、既存の D S P 技術によって本発明に係る計算を、本 F I R フィルタにより実現する高速かつ低消費電力のデバイスが構成できる。

【0 1 8 7】

図 3 は、このようにして構成した F I R フィルタの概要構成を示す模式図である。

【0 1 8 8】

F I R フィルタ 3 0 1 は、チェビシェフ・カオス型の拡散符号系列 X_1 , X_2 , X_3 , ... の入力を、端子 3 0 5 にて受け付ける。

【0 1 8 9】

受け付けられたチェビシェフ・カオス型の拡散符号系列は、直列接続された遅延回路 3 0 2 により、順次遅延されて配送される。遅延時間は、チップ長である。

【0 1 9 0】

また、遅延回路 3 0 2 同士の間順次現れる拡散符号を、増幅器 3 0 3 によって増幅する。増幅率は、本図に示すように、それぞれ、 $(-r)^N$, $(-r)^{N-1}$, $(-r)^{N-2}$, ..., $(-r)^2$, $(-r)^1$ である。

【0 1 9 1】

ここで、 r を「数14」にて定義される実インパルス定数とした場合が最適となるが、「数14」を厳密に満足しなくとも、 $-1 < r < 1$ である限り、非同期CDMA通信システムの拡散符号生成に用いることができる。

【0192】

増幅器303によって増幅された信号は、加算器304によって加算され、最適カオス型拡散符号系列 Y_1, Y_2, Y_3, \dots が順次出力される。

【0193】

今、符号系列が、周期的である場合、すなわち、 $X_j = X_{j+N+1}$ である場合は、 $2N-1$ 個の数値 X_1, \dots, X_{2N-1} を用意する必要はない。 N 個の X_1, \dots, X_N だけあれば、周期性を利用して、すべての m ($0 \leq m \leq N$)に対して、 $B(X_m)$ を計算できる。したがって、さらに計算時間を短縮することができる。

【0194】

同様に、チェビシェフ多項式の積「数45」も s 次元キュービック $[-1, 1]^s$ 上で、完全直交基底となることが解る。

【0195】

【数45】

$$\prod_{j=1}^s T(p_j, x_j) \\ = T_{p_1}(x_1) T_{p_2}(x_2) \cdots T_{p_s}(x_s)$$

【0196】

本発明では、 s 個の所定の正整数 q_1, q_2, \dots, q_s に対して、それぞれ $q_1 \bmod p_1 \neq 0, q_2 \bmod p_2 \neq 0, \dots, q_s \bmod p_s \neq 0$ が成立するような s 個の整数パラメータ p_1, p_2, \dots, p_s で決められるチェビシェフ写像力学系から、それぞれ生成された s 次元の実数値 x_1, x_2, \dots, x_s に対して、 s 個の積「数46」を計算する。

【0197】

【数 4 6】

$$z[m] = T_{q_1}(x_1[m])T_{q_2}(x_2[m]) \cdots T_{q_s}(x_s[m]) \\ (1 \leq m \leq 2N - 1)$$

【0 1 9 8】

すると、計算された値 $z[1]$, $z[2]$, ..., $z[2N-1]$ から構成される長さ N の擬似拡散系列【数 4 7】の相関関数は、【数 1 3】を満足する。

【0 1 9 9】

【数 4 7】

$$\begin{aligned} z'[1] &= \sum_{j=1}^N (-r)^j z[j], \\ z'[2] &= \sum_{j=1}^N (-r)^j z[j+1], \\ &\vdots \\ z'[N] &= \sum_{j=1}^N (-r)^j z[j+N-1] \end{aligned}$$

【0 2 0 0】

よって、【数 1 4】のように r を定義し、符号長 N を十分に長くとれば、 s 次元の直積カオス力学系から作られる擬似乱数列を拡散符号とする非同期CDMAの干渉ノイズの分散は、上記Mazziniの理論により【数 1 5】によって表され、既存の非同期CDMA通信システムの場合より、同一ビット誤り率下で確実に15パーセントのユーザー数を増やすことができる。

【0 2 0 1】

また、チェビシェフ写像 $T_p(x)$ と、微分同相写像 $G(x)$ に対して、【数 4 8】の関係（位相同型）を満足すれば、この $F_p(x)$ も、チェビシェフ写像と同等なルベグスペクトラムを持ち、更に、本自己相関関数が、 $(-r)^l$ の様にダンプする様なカオス系列を、同様に構成することができる。

【0 2 0 2】

【数 48】

$$F_p \circ G(x) = G \circ T_p(x)$$

【0203】

図4、図5は、擬似乱数列の長さNを固定して、ユーザー数Kに対して、本手法、ホワイトノイズ符号、ゴールド符号のそれぞれのビット誤り率を計算したシミュレーション結果である。なお、本手法では、以下のパラメータを用いた。

・ s=1。

・ p=2もしくはp=3（チェビシェフGeneratorの次数は、2または3に相当）

。

【0204】

このシミュレーション結果から、既存の最適系列と考えられていたホワイトノイズ符号、ゴールド符号と比較して、同一ビット誤り率下で、15パーセントのユーザー数を確保することができることがわかる。

【0205】

図6は、符号長N=31、ユーザー数K=7の場合、本結果の計算精度を7ビットから31ビットまで変化させたときのシミュレーション結果である。

【0206】

計算精度が11ビットと比較的低い場合でも、本実施形態による擬似乱数列発生の有効性が現れていることが解る。

【0207】

図7は、符号長N=63で、計算精度を11ビットから31ビットまで変化させた場合の、ユーザー数対ビット誤り率を計算したシミュレーション結果である。

【0208】

計算精度が15ビットと低い場合でも、本擬似乱数列発生の有効性が現れていることが解る。

【0209】

なお、図4から図8に示すシミュレーション結果は、発明者を著者に含む4人の共同研究C. C. Chen, K. Yao, K. Umeno, E. Biglieri「Applications of Cha

otic Dynamical Systems and Ergodic Theory to the Design of Spread Spectrum Sequences」 (preprint submitted to IEEE trans. on Circuits and Systems. submission date: Jan. 31, 2000) として開示される予定である。

【0210】

このようにして、本実施形態により、上記課題を解決することができる。

【0211】

図8は、擬似乱数列の出力装置101において実行される処理、すなわち、本発明の擬似乱数列の出力方法の工程を示すフローチャートである。

【0212】

擬似乱数列の出力装置101は、系列初期値と整数パラメータ（次数）を受け付け（ステップS301）、これらと上記の漸化式に基づいて擬似乱数列を計算し（ステップS302）、計算した擬似乱数列を出力して（ステップS303）、本処理を終わる。

【0213】

このように、本発明の擬似乱数列の出力方法は、汎用コンピュータ、並列コンピュータ、携帯端末、特に通信端末、ゲーム装置などの情報処理装置により容易に実行することができる。

【0214】

また、DSPやFPGA（Field Programmable Gate Array）などのデジタル回路を用いて、本発明の擬似乱数列の出力方法を実行することも容易である。

【0215】

（送信装置の実施形態）

図9は、本発明の送信装置の概要構成を示す模式図である。なお、上記の図と同じ要素には、同じ符号を付してある。以下、本図を参照して説明する。

【0216】

送信装置401は、信号受付部402と、系列出力部403と、拡散部404と、信号送信部405と、を備える。系列出力部403は、擬似乱数列の出力装置101を備えており、これを制御する。

【0217】

信号受付部 4 0 2 は、伝送すべき信号を受け付ける。伝送信号として典型的なものは、携帯電話や P H S の場合には音声信号である。デジタル通信を行う場合には、電氣的なデジタル信号である。光通信を行う場合には、光信号から電気信号への変換を行った上で電気信号を受け付けてもよいし、擬似乱数列の出力装置 1 0 1 を光コンピュータで実現する場合は、光信号をそのまま受け付ける。

【 0 2 1 8 】

系列出力部 4 0 3 は、送信装置 4 0 1 に割り当てられた系列初期値と整数パラメータ（次数）とを、これが備える擬似乱数列の出力装置 1 0 1 に受け付けさせる。擬似乱数列の出力装置 1 0 1 は、上述のように、擬似乱数列を出力するので、系列出力部 4 0 3 は、この擬似乱数列を出力する。

【 0 2 1 9 】

系列初期値と整数パラメータ（次数）とは、送信装置 4 0 1 のそれぞれに異なる値をあらかじめ割り当てることができる。製造番号、機器番号、承認番号などの数値を R O M（Read Only Memory）に記録した通信端末が普及しているが、これと同様に、系列初期値と整数パラメータ（次数）とをあらかじめ R O M に記録しておいて、当該送信装置 4 0 1 が常に同じ系列初期値と整数パラメータ（次数）とを用いるようにすることができる。また、R O M 内に使用する系列初期値と整数パラメータ（次数）とを複数の種類記録しておき、これらを通信ごとにランダムに選択する手法も利用できる。

【 0 2 2 0 】

このような実施形態をとる場合、送信装置 4 0 1 と通信する受信装置では、R O M 内に記録された系列初期値と整数パラメータ（次数）とを何らかの方法で知る必要があるが、送信装置と受信装置とが 1 対になっている場合には、同じ系列初期値と整数パラメータ（次数）とを共有して記録する実施形態をとることができる。

【 0 2 2 1 】

系列初期値と整数パラメータ（次数）の種類が複数ある場合に、送信装置 4 0 1 がいずれを使用しているか、は、後述する相関検波によって調べることができる。また、チェビシェフ多項式に基づく漸化式によって得られるカオス乱数列を

用いて系列初期値を複数用意してもよい。さらに、後述するように、公開鍵暗号の手法を用いて、送信装置 401 と受信装置とで系列初期値と整数パラメータ（次数）を安全に共有することができる。

【0222】

拡散部 404 は、信号受付部 402 が受け付けた伝送信号に、系列出力部 403 が出力した擬似乱数列の要素を順に乗じて直接スペクトラム拡散する。ここで、時刻 t における信号の値を $s(t)$ として、信号 $s(t)$ に系列の要素を順に乗じる」手法について説明する。

【0223】

長さ N の系列の要素を用いる場合には、これと直接スペクトラム拡散のチップ長さ w から、「信号 $s(t)$ に系列の要素を順に乗じる」の周期は、 Nw になる。

【0224】

所定の時刻 t_0 から「信号 $s(t)$ に系列の要素を順に乗じる」場合、信号 $s(t)$ を、必要な品質が得られるようなチップ長さ w で離散化する。たとえば、チップ長さ w ごとに信号 $s(t)$ の値を得る手法や、チップ長さ w の間の信号 $s(t)$ の値の平均を得る手法などが考えられる。ここでは、説明を明確にするため、前者の手法を用いて説明する。

【0225】

チップ長さ w は、受信装置側で伝送信号の情報を必要な品質で十分に復号できるような長さにする必要があるが、公知の技法により、適切なチップ長を選択することができる。

【0226】

また、適切なチップ長さ w を選択すれば、離散化された信号列を順に当該チップ長時間 w だけ出力することにより、元の伝送信号から見て十分な品質の信号を得ることができる。

【0227】

離散化された信号は、以下のような数列で表現することができる。

$$s(t_0), s(t_0+w), s(t_0+2w), s(t_0+3w), s(t_0+4w), \dots$$

【0228】

これは、整数 i ($0 \leq i$)について

$$s_i = s(t_0 + iw)$$

と整理することができる。

【0229】

なお、チップ長 w の間の信号 $s(t)$ の値の平均をとる手法では、以下のよう
に整理することができる。

$$s_i = (1/w) \int_0^w s(t_0 + iu) du$$

【0230】

これらの信号列 s_i ($0 \leq i$)は、必要な品質で伝送信号を離散化したものである

。

【0231】

この信号列を、直接スペクトラム拡散した後の信号列は、

$$s_0 z'[1], s_1 z'[2], \dots, s_{N-1} z'[N], s_N z'[1], s_{N+1} z'[2], \dots$$

のようになる。

【0232】

すなわち、整数 i ($0 \leq i$)に対して、 $s_i \times z'[(i \bmod N) + 1]$ が、この数列の一般
項である。ここで、 $x \bmod y$ は、 x を y で割った余りを意味する。

【0233】

この信号列の要素を、それぞれチップ長の時間だけ送信することにより、受け
付けられた所定の時間長の伝送信号を同じ時間長で送信することができる。

【0234】

図10には、直接スペクトラム拡散処理の様子を示す。信号受付部402が受
け付けた伝送信号501に対して、系列出力部403が出力した擬似乱数列50
2の要素を繰り返し乗ずることにより、拡散部404が出力する信号503が得
られる。

【0235】

信号送信部405は拡散部404が出力する信号503を送信する。送信は、
たとえば、携帯電話やPHSの場合はアンテナを介して、コンピュータ通信網の
場合は有線の電話回線や有線／無線LAN回線を介して、あるいは光ケーブルを

介して行われる。

【0236】

(受信装置の実施形態)

本発明の受信装置は、上記の送信装置同様、上記の擬似乱数列の出力装置を用いて擬似乱数列を得て、これを直接スペクトラム逆拡散用の拡散符号として用いる。図11は、本発明の受信装置の概要構成を示す模式図である。以下、本図を参照して説明する。

【0237】

受信装置601は、信号受信部602と、系列出力部604と、逆拡散部605と、を備える。

【0238】

信号受信部602は、上記の送信装置401により送信された信号を受信する。信号受信部602は、たとえば、アンテナ、電話回線や光ケーブル回線などに対するインターフェースにより実現される。

【0239】

信号受信部602が受信する信号には、通信相手以外の送信装置401が送信した信号や、ノイズが含まれている。これら不要な信号を除去するために、通信相手の送信装置401が直接スペクトラム拡散に用いた擬似乱数列と同じ擬似乱数列を用いる。系列出力部604は、通信相手の送信装置401が用いた系列初期値と整数パラメータ（次数）と、を上記の擬似乱数列の出力装置101に受け付けさせることにより、この擬似乱数列を出力する。したがって、受信装置601の系列出力部604の実施態様は、送信装置401の系列出力部403と同様である。

【0240】

通信相手の送信装置401が受け付けた伝送信号を復号するには、通信相手の送信装置401が送信した信号に対して、擬似乱数列の要素の逆数を順に乗じて直接スペクトラム逆拡散すればよい。同期が取れていれば、受信した信号列

$$s_0z'[1], s_1z'[2], \dots, s_{N-1}z'[N], s_Nz'[1], s_{N+1}z'[2], \dots$$

に、擬似乱数列の要素の逆数

$1/z'[1], 1/z'[2], \dots, 1/z'[N]$

を順に乗ずることにより、伝送信号の情報を必要な品質で復号した信号列

$s_0, s_1, \dots, s_{N-1}, s_N, s_{N+1}, \dots$

が得られる。この信号列を、それぞれチップ長時間 w だけ順に出力すれば、伝送信号が必要な品質で復元できるのである。

【0 2 4 1】

同期には、後述する相関検波のほか、クロックを共有する手法など、各種の手法が考えられ、これらの実施形態も本発明の範囲に含まれる。

【0 2 4 2】

以下のように、送信装置 4 0 1 と受信装置 6 0 1 とで通信を行う公開鍵暗号の手法を用いて、受信装置の生成部 6 1 1 は、送信装置 4 0 1 と同じ系列初期値および整数パラメータ（次数）を生成することができる。

【0 2 4 3】

まず、受信装置 6 0 1 は、公開鍵と秘密鍵の対を生成する。次に、受信装置 6 0 1 は、送信装置 4 0 1 に対して公開鍵を送信する。送信装置 4 0 1 は、自ら使用する系列初期値および整数パラメータ（次数）を当該公開鍵で暗号化して受信装置 6 0 1 に送信する。受信装置 6 0 1 は、送られた暗号を秘密鍵で復号し、系列初期値および整数パラメータ（次数）を得る。

【0 2 4 4】

このような公開鍵暗号の手法として、本発明の発明者が特願平 1 1 - 1 5 2 0 6 3 号に開示するようなカオス暗号を用いることができる。

【0 2 4 5】

（相関検波の実施形態）

送信装置 4 0 1 で、複数の擬似乱数列からいずれかを選択して直接スペクトラム拡散した場合、受信装置 6 0 1 は、相関検波により、選択された擬似乱数列を知得することができる。また、相関検波により、直接スペクトラム逆拡散のための同期をとることができる。

【0 2 4 6】

以下、図 1 2 を参照して、相関検波を行う場合の受信装置の実施形態について

説明する。なお、図 12 では、上記の図に示す要素と同じものには同じ符号を付している。

【0247】

受信装置 601 は、信号受信部 602 と、系列出力部 604 と、逆拡散部 605 と、のほか、生成部 611 と、相関検波部 612 を備える。

【0248】

生成部 611 は、送信装置 401 で選択可能な系列初期値と整数パラメータ（次数）の組を出力する。擬似乱数列を 1 つだけ出力してもよい。この場合、相関検波部 612 は、複数の系列初期値と整数パラメータ（次数）の組からいずれか 1 つの組を選択する必要はないため、信号の同期をとるために機能する。

【0249】

系列出力部 604 は、生成部 611 が生成する系列初期値と整数パラメータ（次数）に応じて、送信装置 401 で選択可能な擬似乱数列をそれぞれ出力する。

【0250】

相関検波部 612 では、系列出力部 604 が出力する擬似乱数列のそれぞれについて相関検波を試みる。調べたい擬似乱数列の「要素」を順に受信した信号に乘ずることにより、相関検波を行う。相関検波の手法については公知の技法を用いることができる。

【0251】

本発明で用いる擬似乱数列は、相関特性に優れているため、受信装置 601 で異なる擬似乱数列を選択した場合には、乗じた後の信号の強度が極めて弱くなり、相関検波に失敗する。

【0252】

一方、送信装置 401 の擬似乱数列と同じものを選択して相関検波を行った場合は、乗じた後の信号の強度が所定の値を超えることになる。また、受信信号に同期するように擬似乱数列のオフセットを移動して信号の同期をとることができる。

【0253】

逆拡散部 605 は、信号受信部 602 により受信された信号に、相関検波部 6

12により選択されて当該受信された信号に同期された擬似乱数列の「要素の逆数」を順に乗じて、伝送信号を復号する。

【0254】

受信された信号に対して、相関検波部612では擬似乱数列の「要素」を順に乗ずるのに対し、逆拡散部605では擬似乱数列の「要素の逆数」を順に乗ずる点異なる。前者では、自己相関、相互相関を計算するのに対し、後者では、復号が行われるのである。

【0255】

(通信システム)

本発明の通信システムは、上記の送信装置401と、これが送信する信号を受信して伝送信号を復号する上記の受信装置601と、から構成することができる。これらの送信装置401と受信装置601で、使用する擬似乱数列が異なれば伝送信号の復号に失敗する。

【0256】

したがって、複数の送信装置401と複数の受信装置601とが同じ周波数帯で通信していても、秘話性を保つとともに、使用している通信者の対の数に応じた品質を保証して、相互に通信を行うことができる。

【0257】

特に、本発明にて生成される擬似乱数列では、従来の擬似乱数列に比較して符号の種類を格段に増やすことができるため、潜在的に多数のユーザを含むようなCDMA方式の通信に適している。

【0258】

【発明の効果】

以上説明したように、本発明によれば、非同期CDMA通信システムにて拡散符号として用いるのに好適な擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置、擬似乱数列の出力方法、送信方法、受信方法、フィルタ方法、ならびに、情報記録媒体を提供することができる。

【図面の簡単な説明】

【図1】

本発明の擬似乱数列の出力装置の概要構成を模式図である。

【図 2】

チェビシェフ写像の概要を示すグラフである。

【図 3】

本実施形態にて利用可能な F I R フィルタの概要構成を示す模式図である。

【図 4】

本手法と従来の手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 5】

本手法と従来の手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 6】

本手法にて計算精度を変化させた場合のシミュレーション結果を示すグラフである。

【図 7】

本手法にて計算精度を変化させた場合のシミュレーション結果を示すグラフである。

【図 8】

本発明の擬似乱数列の出力方法の工程を示すフローチャートである。

【図 9】

本発明の送信装置の概要構成を示す模式図である。

【図 1 0】

直接スペクトル拡散の様子を示す説明図である。

【図 1 1】

本発明の受信装置の概要構成を示す模式図である。

【図 1 2】

関連検波を行う場合の受信装置の実施形態について示す模式図である。

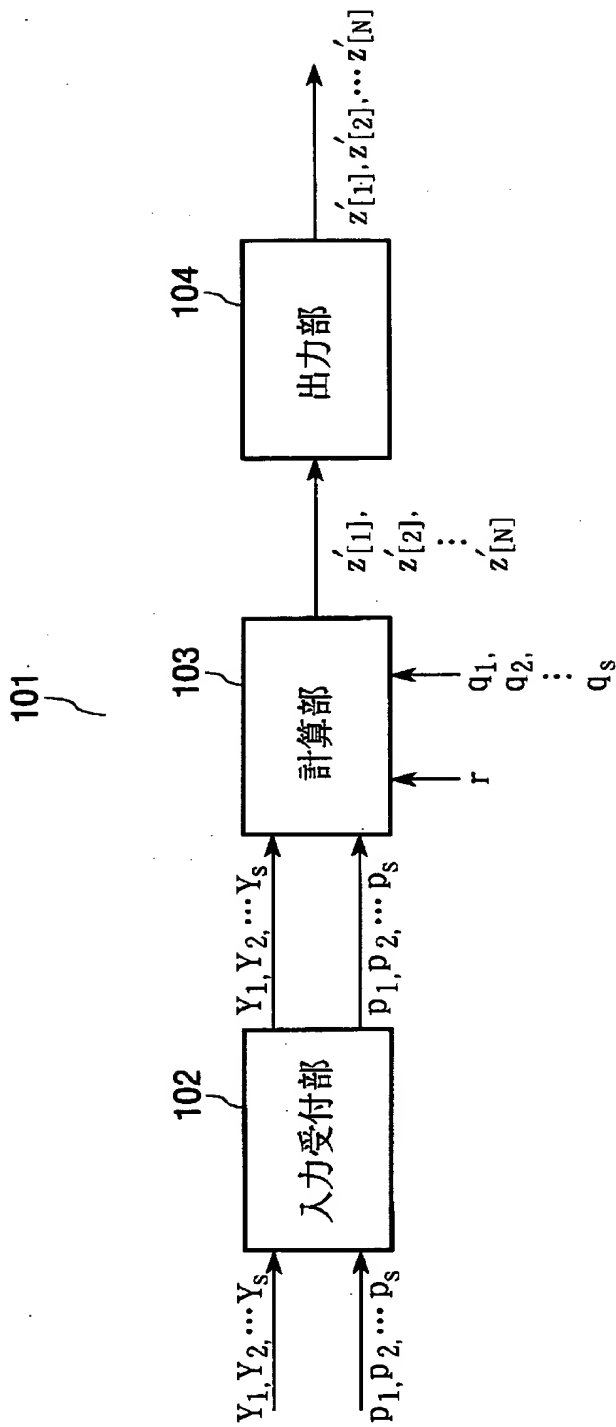
【符号の説明】

1 0 1 擬似乱数列の出力装置

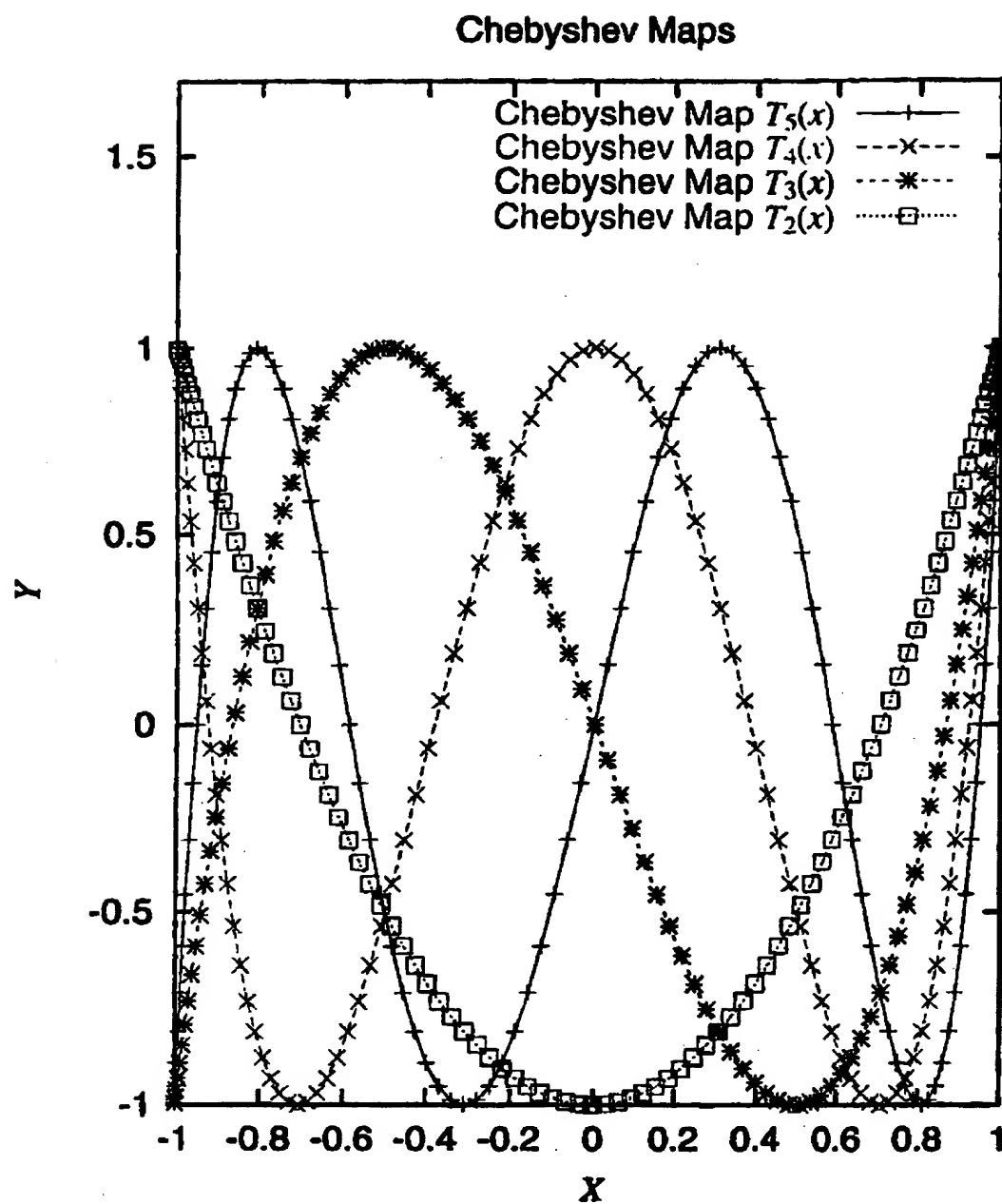
- 1 0 2 入力受付部
- 1 0 3 計算部
- 1 0 4 出力部
- 3 0 1 F I R フィルタ
- 3 0 2 遅延回路
- 3 0 3 増幅器
- 3 0 4 加算器
- 3 0 5 端子
- 4 0 1 送信装置
- 4 0 2 信号受付部
- 4 0 3 系列出力部
- 4 0 4 拡散部
- 4 0 5 信号送信部
- 5 0 1 伝送信号
- 5 0 2 擬似乱数列
- 5 0 3 出力信号
- 6 0 1 受信装置
- 6 0 2 信号受信部
- 6 0 4 系列出力部
- 6 0 5 逆拡散部
- 6 1 1 生成部
- 6 1 2 相関検波部

【書類名】 図面

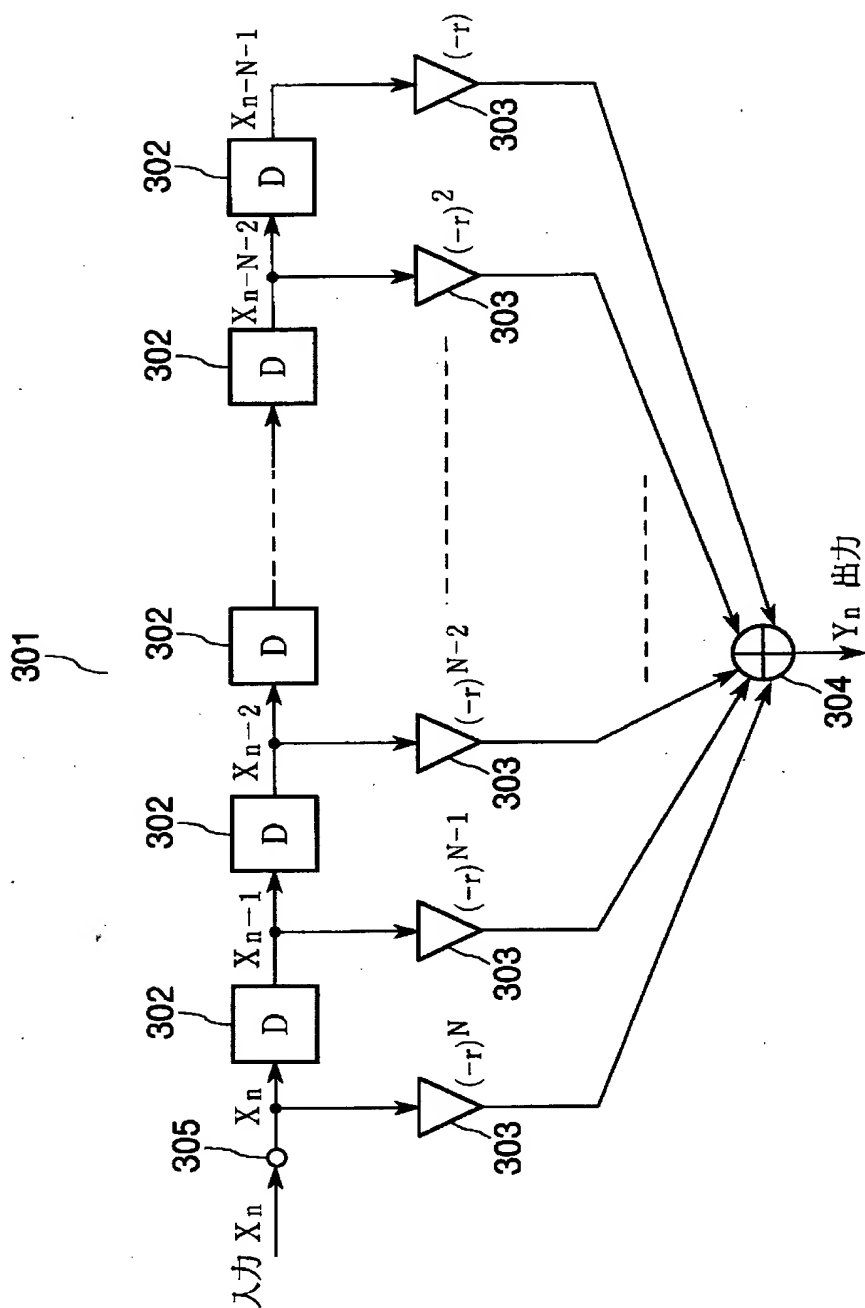
【図 1】



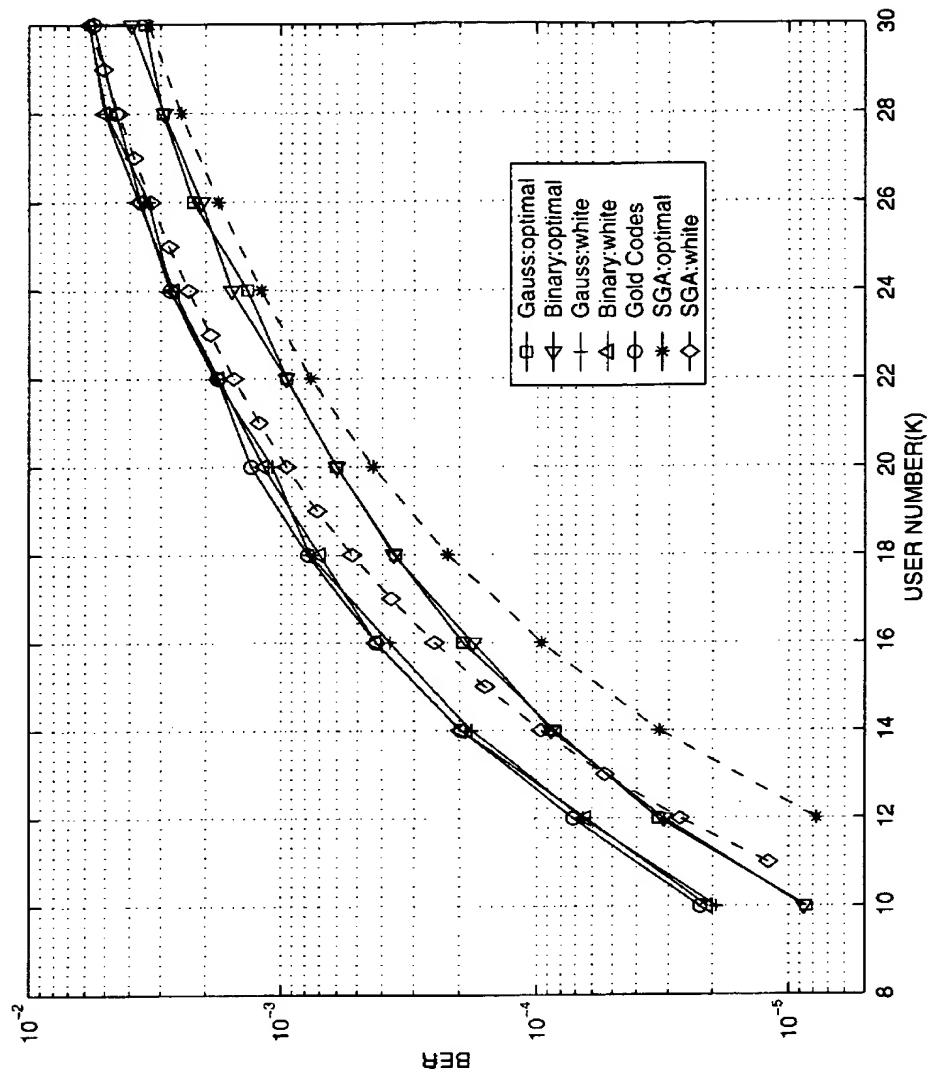
【図 2】



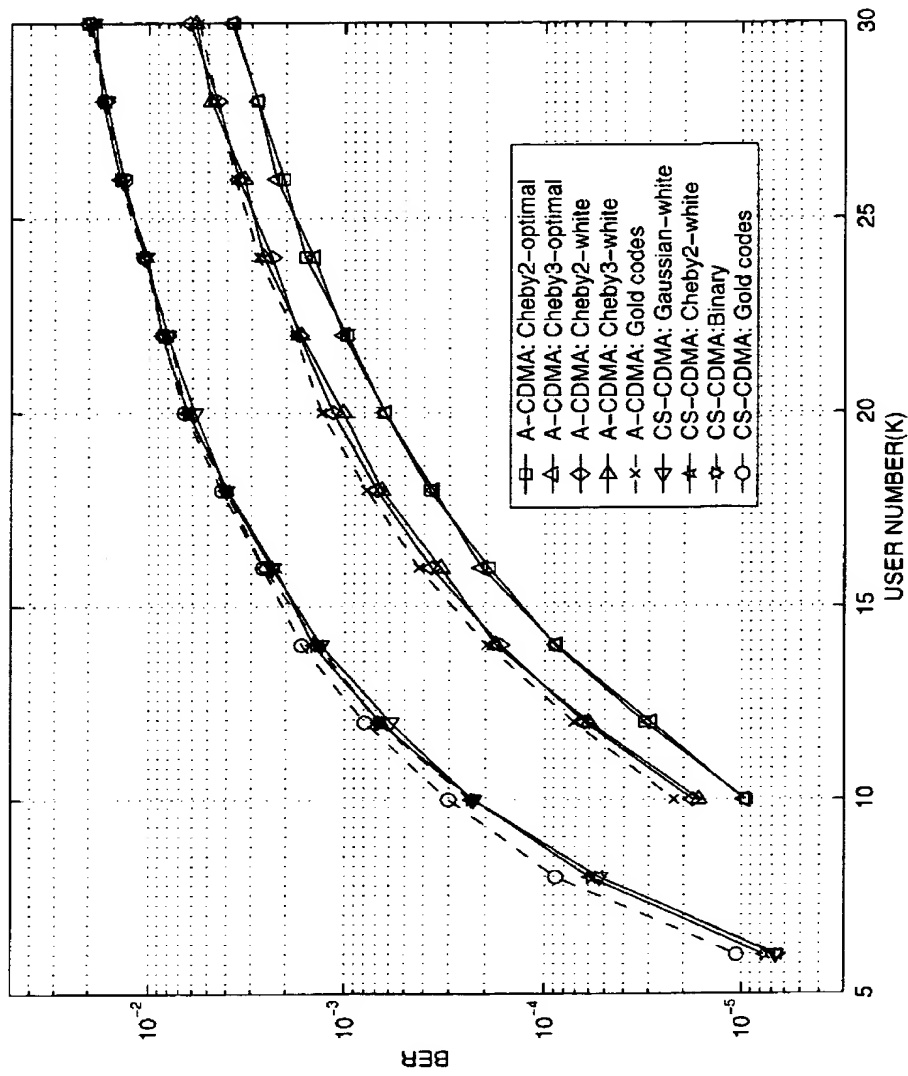
【図 3】



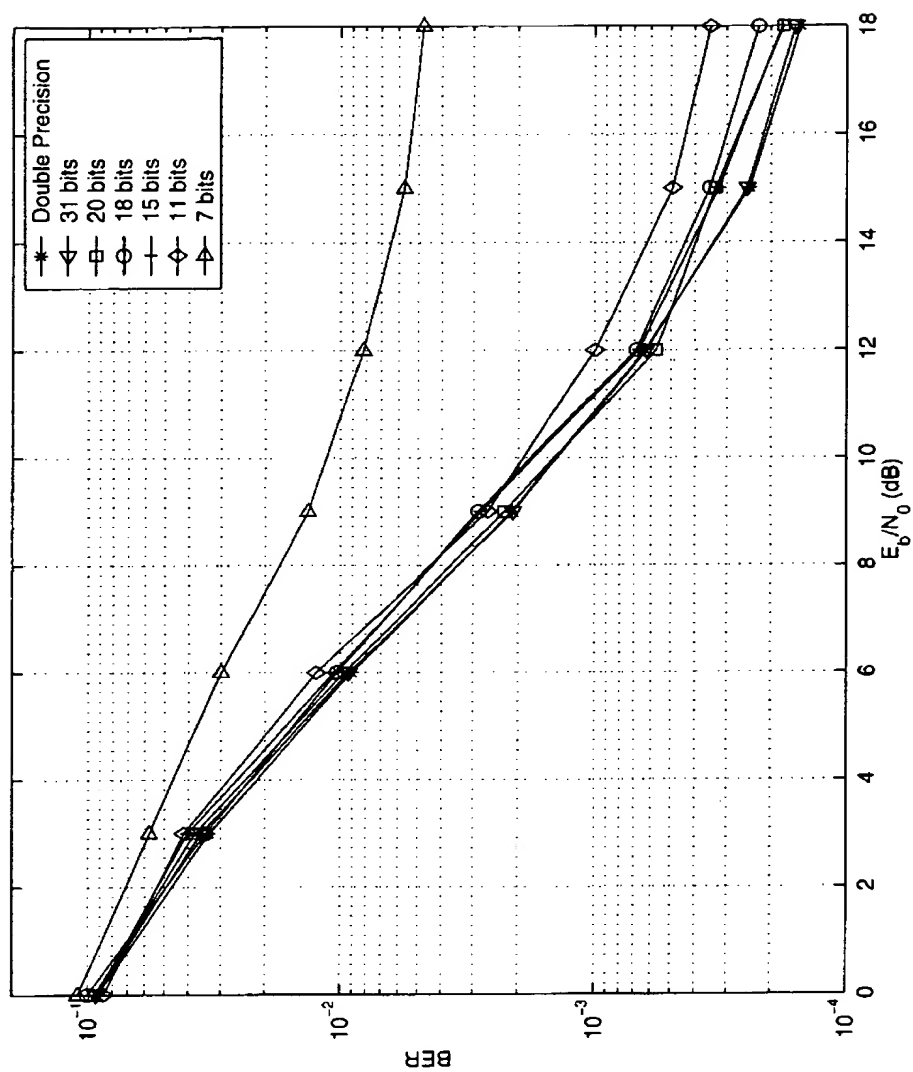
【図 4】



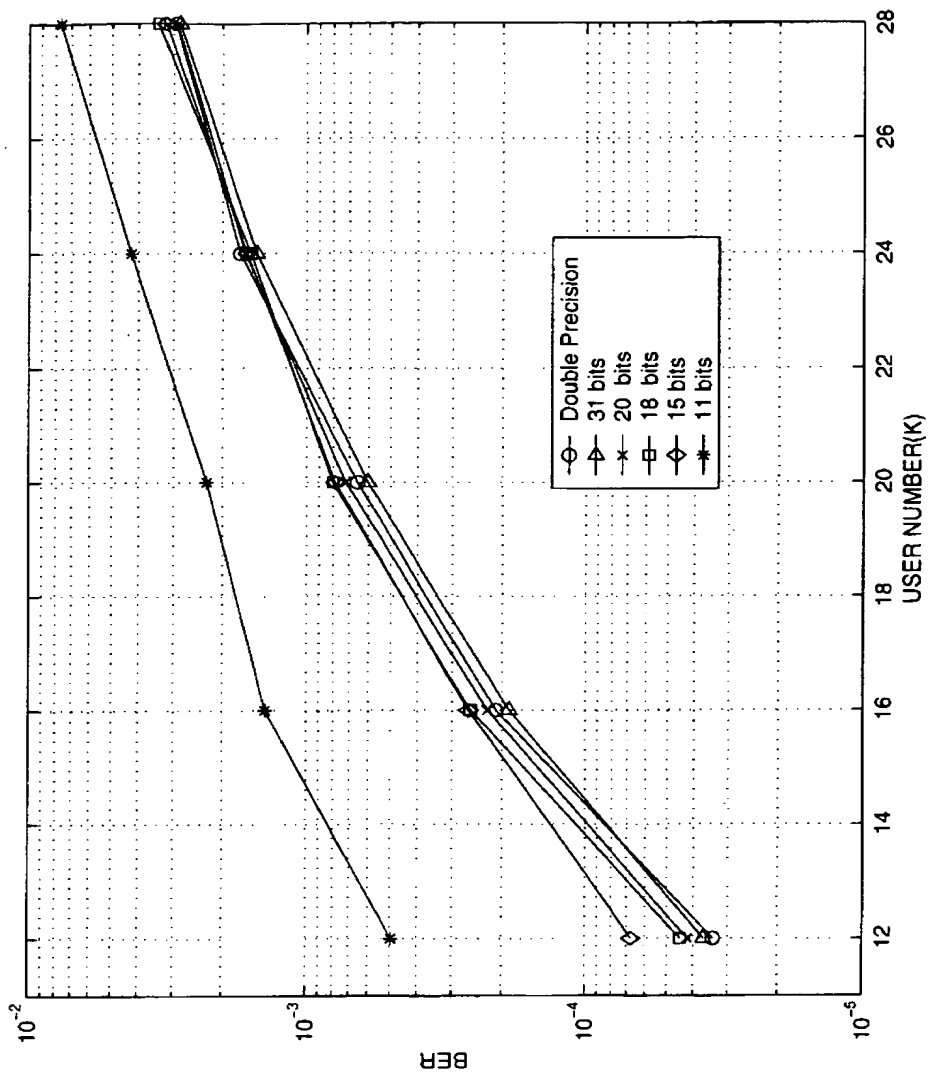
【図 5】



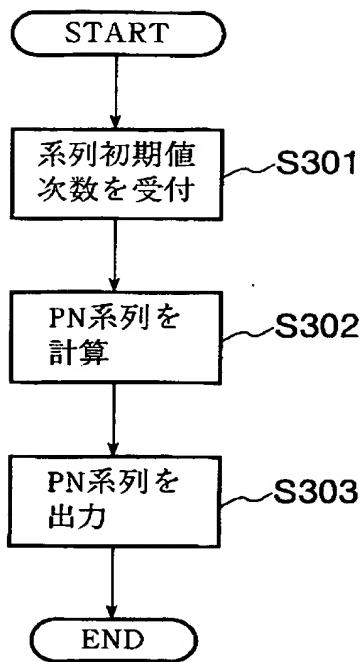
【図6】



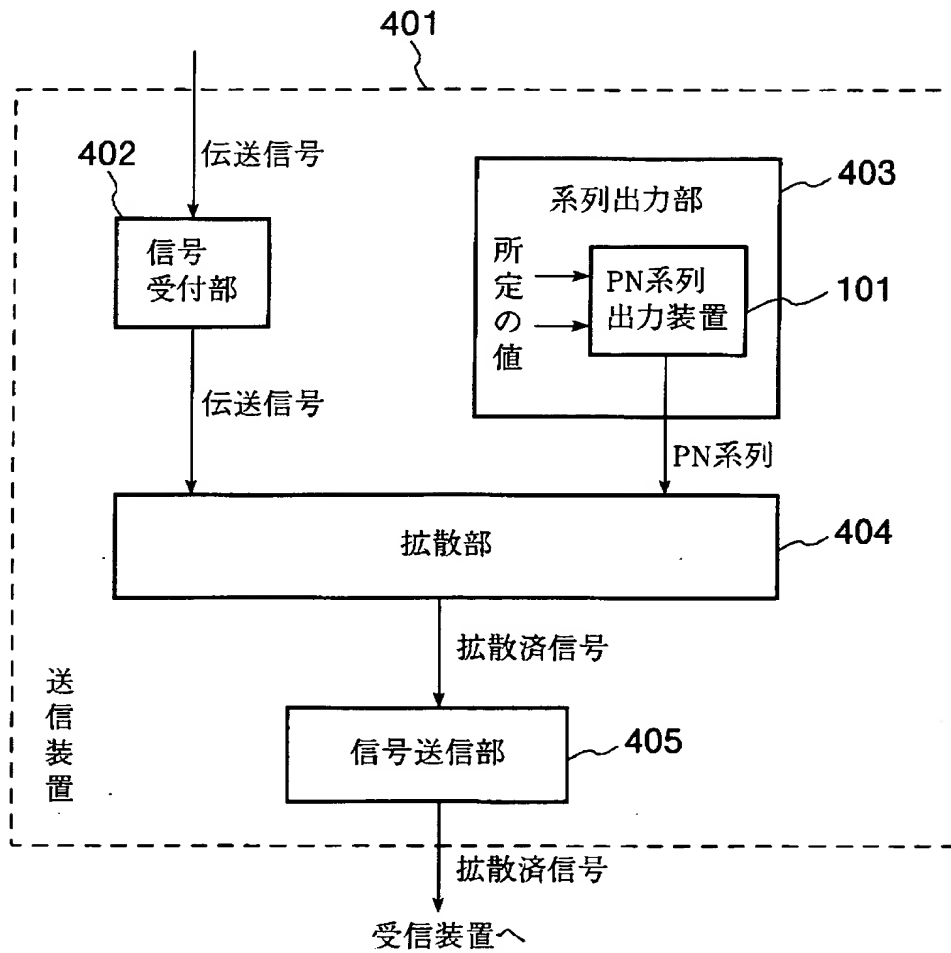
【図 7】



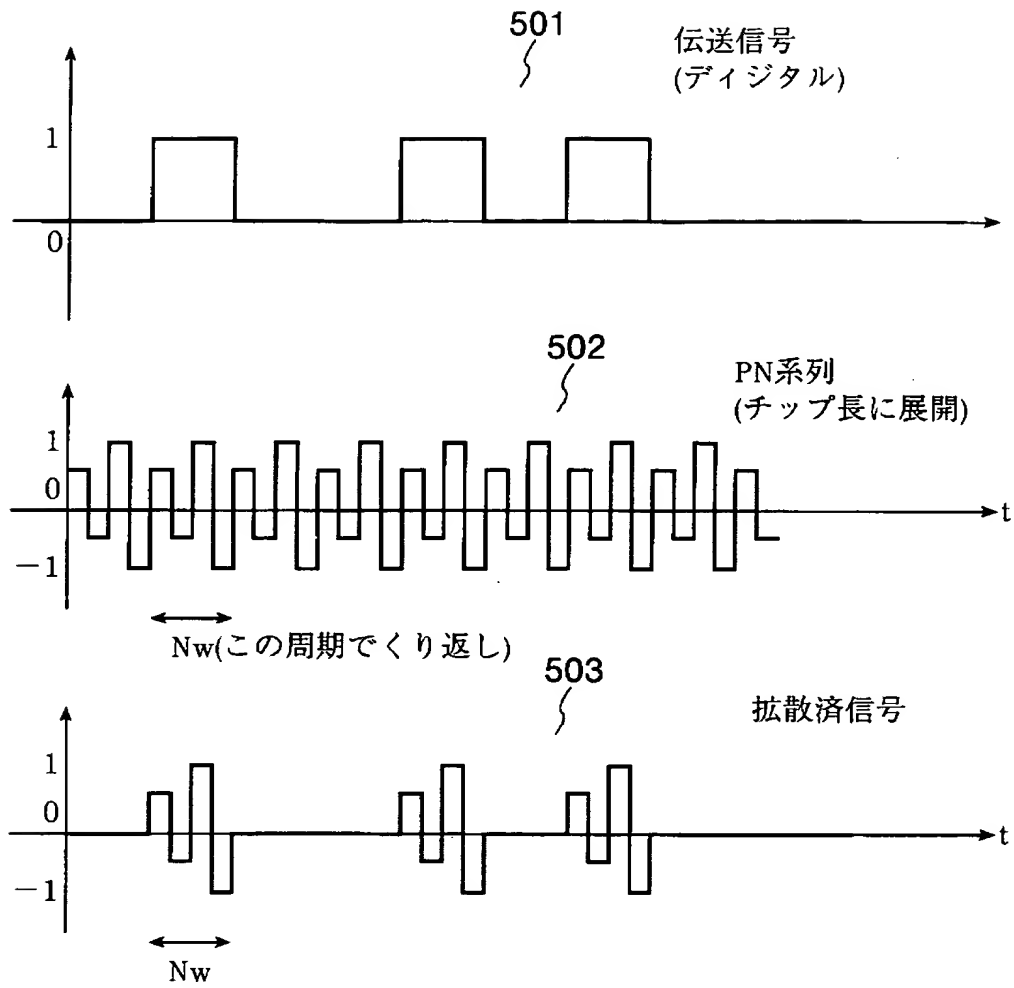
【図 8】



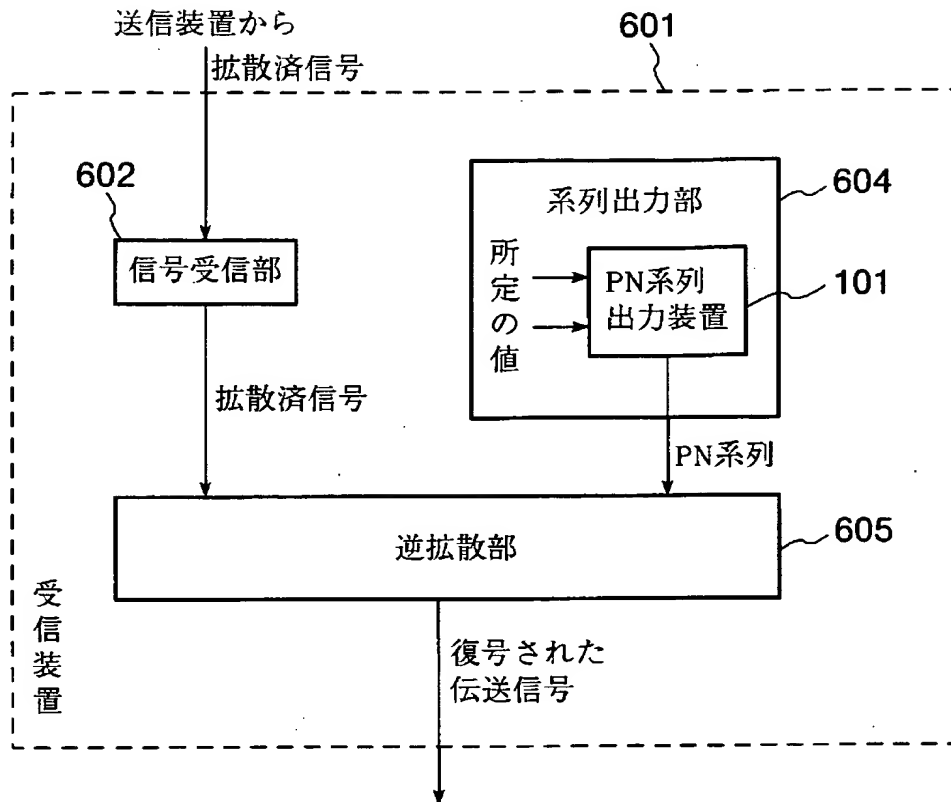
【図 9】



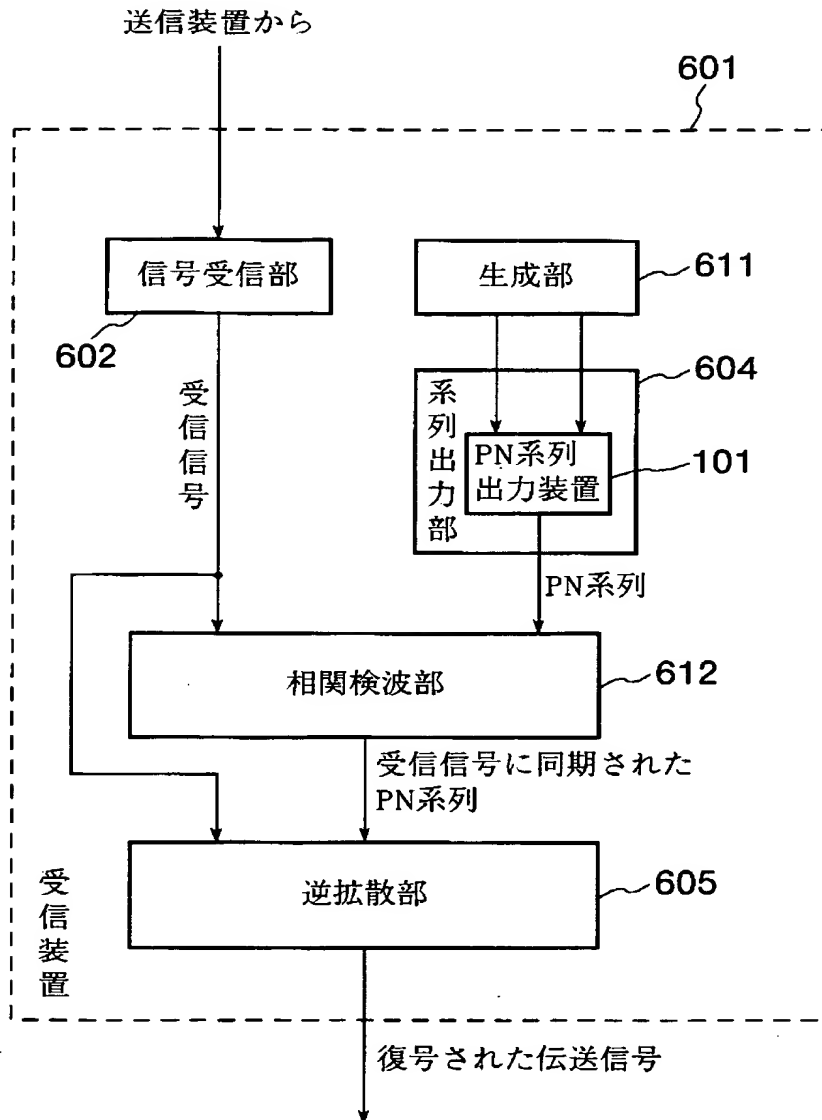
【図 1 0】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 非同期 C D M A 通信システムにて拡散符号として用いるのに好適な擬似乱数列を生成するフィルタ装置等を提供する。

【解決手段】 所定の実インパルス定数 r ($-1 < r < 1$) に対する F I R フィルタ 3 0 1 は、チップ長 D のチェビシェフ・カオス型の拡散符号系列の入力信号の入力を端子 3 0 5 で受け付け、入力信号を、それぞれ 0 、 D 、 $2D$ 、 $3D$ 、 \dots 、 $(N-1)D$ だけ遅延させた複数の信号を遅延回路 3 0 2 により出力し、遅延されて出力された複数の信号のそれぞれの、当該遅延時間が T である場合、増幅器 3 0 3 により $(-r)^{(N-T)/D}$ 倍して出力し、増幅されて出力された複数の信号の総和、すなわち、最適カオス型拡散符号系列を、加算器 3 0 4 により出力する。

【選択図】 図 3

認定・付加情報

特許出願の番号	特願 2000-107047
受付番号	50000445549
書類名	特許願
担当官	塩崎 博子 1606
作成日	平成12年 6月19日

<認定情報・付加情報>

【特許出願人】

【識別番号】	391027413
【住所又は居所】	東京都小金井市貫井北町4丁目2番1号
【氏名又は名称】	郵政省通信総合研究所長

【特許出願人】

【識別番号】	597044841
【住所又は居所】	東京都小金井市貫井北町4丁目2番地1号 郵政 省通信総合研究所内

【氏名又は名称】	梅野 健
----------	------

【代理人】

申請人

【識別番号】	100095407
【住所又は居所】	東京都千代田区神田錦町2丁目7番地 協販ビル 7階 芦田・木村国際特許事務所

【氏名又は名称】	木村 満
----------	------

【選任した代理人】

【識別番号】	100110135
【住所又は居所】	東京都千代田区神田錦町2丁目7番地 協販ビル 7階 芦田・木村国際特許事務所

【氏名又は名称】	石井 裕一郎
----------	--------

次頁無

【書類名】 出願人名義変更届（一般承継）

【提出日】 平成13年 2月 5日

【あて先】 特許庁長官 殿

【事件の表示】

【出願番号】 特願2000-107047

【承継人】

【識別番号】 301001775

【氏名又は名称】 総務省通信総合研究所長 飯田 尚志

【承継人代理人】

【識別番号】 100082669

【弁理士】

【氏名又は名称】 福田 賢三

【提出物件の目録】

【物件名】 権利の承継を証明する書面 1

【援用の表示】 平成 1 3 年 2 月 5 日提出の特願 2 0 0 0 - 1 5 4 1 7 6
出願人名義変更届（一般承継）に添付のものを援用する
。

【物件名】 委任状 1

【援用の表示】 平成 1 3 年 2 月 5 日提出の特願 2 0 0 0 - 1 5 4 1 7 6
出願人名義変更届（一般承継）に添付のものを援用する
。

【プルーフの要否】 要

認定・付加情報

特許出願の番号	特願 2000-107047
受付番号	50100152559
書類名	出願人名義変更届（一般承継）
担当官	末武 実 1912
作成日	平成13年 3月21日

<認定情報・付加情報>

【承継人】

【識別番号】	301001775
【住所又は居所】	東京都小金井市貫井北町4-2-1
【氏名又は名称】	総務省通信総合研究所長

【承継人代理人】

申請人	
【識別番号】	100082669
【住所又は居所】	東京都港区西新橋1-6-13 柏屋ビル
【氏名又は名称】	福田 賢三

次頁無

【書類名】 出願人名義変更届（一般承継）

【提出日】 平成13年 5月10日

【あて先】 特許庁長官 殿

【事件の表示】

【出願番号】 特願2000-107047

【承継人】

【識別番号】 301022471

【氏名又は名称】 独立行政法人通信総合研究所

【承継人代理人】

【識別番号】 100082669

【弁理士】

【氏名又は名称】 福田 賢三

【提出物件の目録】

【物件名】 権利の承継を証明する書面 1

【援用の表示】 平成13年5月10日提出の特願2000-154176 出願人名義変更届（一般承継）に添付のものを援用する。

【物件名】 委任状 1

【援用の表示】 平成13年5月10日提出の特願2000-154176 出願人名義変更届（一般承継）に添付のものを援用する。

【プルーフの要否】 要

認定・付加情報

特許出願の番号	特願 2000-107047
受付番号	50100671041
書類名	出願人名義変更届 (一般承継)
担当官	末武 実 1912
作成日	平成 13 年 6 月 18 日

< 認定情報・付加情報 >

【承継人】

【識別番号】	301022471
【住所又は居所】	東京都小金井市貫井北町 4-2-1
【氏名又は名称】	独立行政法人通信総合研究所

【承継人代理人】

申請人	
【識別番号】	100082669
【住所又は居所】	東京都港区西新橋 1-6-13 柏屋ビル
【氏名又は名称】	福田 賢三

次頁無

特願 2 0 0 0 - 1 0 7 0 4 7

出 願 人 履 歴 情 報

識別番号 [3 9 1 0 2 7 4 1 3]

1. 変更年月日	1 9 9 1 年 3 月 1 1 日
[変更理由]	新規登録
住 所	東京都小金井市貫井北町 4 丁目 2 番 1 号
氏 名	郵政省通信総合研究所長

特願 2000-107047

出願人履歴情報

識別番号 [597044841]

1. 変更年月日 1999年10月27日
[変更理由] 住所変更
住 所 東京都小金井市貫井北町4丁目2番地1号 郵政省通信総合研
究所内
氏 名 梅野 健
2. 変更年月日 2001年 6月20日
[変更理由] 住所変更
住 所 東京都小金井市貫井北町4-2-1 独立行政法人通信総合研
究所内
氏 名 梅野 健

特願 2 0 0 0 - 1 0 7 0 4 7

出 願 人 履 歴 情 報

識別番号 [3 0 1 0 0 1 7 7 5]

1. 変更年月日	2 0 0 1 年 1 月 1 2 日
[変更理由]	新規登録
住 所	東京都小金井市貫井北町 4 - 2 - 1
氏 名	総務省通信総合研究所長

特願 2 0 0 0 - 1 0 7 0 4 7

出 願 人 履 歴 情 報

識別番号

[3 0 1 0 2 2 4 7 1]

1. 変更年月日 2 0 0 1 年 4 月 2 日
[変更理由] 新規登録
住 所 東京都小金井市貫井北町 4 - 2 - 1
氏 名 独立行政法人通信総合研究所
2. 変更年月日 2 0 0 4 年 4 月 1 日
[変更理由] 名称変更
住 所 東京都小金井市貫井北町 4 - 2 - 1
氏 名 独立行政法人情報通信研究機構